Scam mobile messages: guidance on protecting people and businesses

Guidance

Published 15 July 2026
Applies from: 18 January 2027 (Person-to-Person messages) / 15 July 2027 (Application-to-Person messages)

Contents

Section

1. Overview

1.1 Organised criminals around the world target people and businesses in the UK with scam mobile messages to elicit a response and pressure or manipulate potential victims into making payments or revealing sensitive information.

1.2 Ofcom has powers under the Communications Act 2003 (the Act) to ensure that telecoms services, such as mobile messaging services, are used effectively and efficiently and are not misused, for example to facilitate fraud or scams.

1.3 Ofcom has introduced rules to reduce the risk that people and businesses receive scam Person-to-Person (P2P)[1] and Application-to-Person (A2P) messages.[2] These rules are set out in General Condition (GC) C9 and Non-Provider Condition 3.[3] The rules are intended to prevent scammers from accessing mobile messaging services and, where they have gained access, to stop them from sending mobile messages.

The purpose of this guidance

1.4 This document constitutes guidance to assist mobile operators, aggregators and other persons that may not fall under these two categories but nonetheless hold numbers[4] to comply with the requirements of GC C9 and Non-Provider Condition 3, as applicable. We will keep this guidance under review and may update it periodically.[5]

1.5 While this guidance is not legally binding, we expect to take it into account when deciding whether to open an investigation into a provider's compliance with GC C9 or Non-Provider Condition 3, relating to the implementation and ongoing operation of their anti-scam measures for mobile messaging services. If we do decide to open such an investigation, we would also take this guidance into account when deciding what type of action may be appropriate.

1.6 This guidance is not exhaustive with respect to how providers should comply with our rules. We expect providers to use it as a framework for how we might interpret the steps they take to comply with GC C9 and Non-Provider Condition 3. We also expect providers to take steps to comply that are reasonable and proportionate for their circumstances and we require them to maintain certain records to demonstrate their compliance.

[1] In our General Conditions, we define 'Person-to-Person Message' or 'P2P Message' as a message sent from one SIM to another, using a Mobile Communications Service or otherwise using a Public Electronic Communications Service.
[2] In our General Conditions, we define 'Application-To-Person Message' or 'A2P Message' as a message from a Business Sender, sent (either directly or indirectly) to Mobile Numbers using a software application and using a Public Electronic Communications Service and/or Public Electronic Communications Network.
[3] Ofcom, 2026. The new GC C9 and Non-Provider Condition 3 are set out in full in Annex 1 and Annex 2 to our July 2026 Statement and will be incorporated into our General Conditions of Entitlement on the date they become effective.
[4] See paragraphs 1.11-1.12 below for further detail.
[5] Whether we consult on changes to the guidance will depend on the nature of the update: for example, we may not consult on changes that update the guidance to update examples of sources of scam reports or to identify new or other relevant legislation or guidance issued by the Information Commissioner's Office.

1.7 Section 3, below, explains the range of powers we have to take enforcement action in the event of a breach of our GCs relating to scam mobile messages (including GC C9) or Non-Provider Condition 3.

1.8 The relevant GCs are set out in full in the consolidated GCs and, for ease, in section 2 below. Where relevant, we also identify the corresponding Non-Provider Condition.

1.9 This guidance document also includes a number of defined terms with which readers may not be familiar. These terms are set out in the consolidated GCs (or Non-Provider Conditions) and we use some in this document for consistency.

Who this guidance applies to

1.10 This guidance applies to providers involved in P2P and A2P messaging, as specified in GC C9 and Non-Provider Condition 3. The rules each provider will need to comply with are specific to the provider's role in the delivery of mobile messages, the channels over which these mobile messages are sent and whether the provider assigns mobile numbers to customers.

1.11 GC C9 and Non-Provider Condition 3 refer to firms within the scope of the specific Conditions as 'Regulated Providers', although for ease we refer in this document to "providers". Different Conditions apply to different types of providers. For the purposes of the GCs, the types of providers to which different individual Conditions apply include:

- Mobile network operators (MNOs), meaning mobile providers that operate their own mobile networks.
- Mobile operators, meaning both MNOs and different types of Mobile Virtual Network Operators (MVNOs), as applicable. MVNOs are mobile providers that do not own the wireless network infrastructure over which they provide mobile services to their customers. They include:
    - 'Thick' MVNOs, which for the purposes of GC C9 and our guidance mean those MVNOs that use their own Short Message Service Centres (SMSCs)[6] to transfer and terminate messages.
    - 'Thin' MVNOs, which for the purposes of GC C9 and our guidance mean those MVNOs that do not have their own SMSC and rely on their host MNO to transfer and terminate messages.
- Aggregators, meaning providers that contract with business senders, Messaging Service Providers (MSPs)[7] and other aggregators to arrange for the delivery of large volumes of A2P messages. They include:

[6] An SMSC is the core network infrastructure responsible for storing and routing SMS messages between end-users' mobile devices, or between businesses and end-users.

[7] MSPs are companies that specialise in interfacing directly with business senders. MSPs often provide an Application Programming Interface that enables business senders to access different messaging services online and may generate messages on the business sender's behalf. MSPs may pass messages to aggregators and terminating mobile operators or enable senders to initiate messages with these providers through their platform. Where we refer to MSPs in this guidance, we are referring to business messaging providers that are either (a) not providing an Electronic Communication Service (ECS) or Electronic Communication Network (ECN) and therefore not a regulated communications provider for the purposes of any of our GCs; or (b) are acting in a capacity where their business sender customers must also sign up with a third-party aggregator, which will subsequently bill the business sender for messages they send.

- Tier 1 aggregators, meaning aggregators that have a direct contractual relationship with a mobile operator to purchase message termination (either directly, or indirectly through an interconnect arrangement).
- Lower-tier aggregators, meaning aggregators that act in a capacity in which they do not contract directly with a Mobile Service Provider that directly terminates A2P messages to recipients. This includes aggregators that contract directly with business senders and subsequently bill the business sender for messages they send.

1.12 We use the word "provider" to refer to both:

- Operators that are a 'Communications Provider' within the scope of GC C9, as defined in the GCs as meaning "a person who (within the meaning of section 32(4) of the Act) provides an electronic communications network or an electronic communications service".
- Other operators that have access to numbers through their number allocations and that, for whatever reason, may not be considered a 'Communications Provider' within the scope of GC C9 in a specific context, but which are within the scope of Non-Provider Condition 3.

Scam prevention measures not covered by our rules

1.13 GC C9 and Non-Provider Condition 3 set out the minimum measures to protect end-users from scam mobile messages that providers must take, but providers may take additional measures beyond those set out in the Conditions or in this guidance. For example, providers may carry out other monitoring based on their review of messages on their network that have not been reported by end-users or third parties, e.g. based on probabilistic search methods[8] that indicate suspicious behaviour. Our rules do not require or prevent this form of monitoring, although we note that it is likely to be considered more intrusive and providers should therefore ensure they comply with other relevant legislation.

Other relevant legislation

1.14 In using this guidance (or implementing scam prevention measures more generally), providers should ensure they comply with relevant data protection legislation, discussed in more detail in paragraphs 2.248-2.260 below.

1.15 Providers should also ensure they comply with their obligations under other relevant legislation. This may include consumer law (including under the Consumer Rights Act 2015 and the Digital Markets, Competition and Consumers Act 2024) and the Investigatory Powers Act 2016 (relating, amongst other things, to the acquisition and retention of communications data). Providers may also want to consider the Guiding Principles on

[8] Probabilistic search methods involve making decisions on how to process mobile messages based on the likelihood that they might harm the recipient. They can include reviewing messages for a broad set of scam indicators, e.g. phrases such as "Hi Mum …". By contrast, our measures require providers to review messages for known scam numbers or URLs (in effect, our measures should require providers to implement a database matching tool, where a human sets a rule that is applied automatically).

Business and Human Rights,[9] which explains how businesses can avoid infringing on the human rights of others and address any adverse human rights impacts of their activities.

Overview of our rules

1.16 Table 1 summarises the main requirements set out in GC C9 and to whom they would apply.[10] Where applicable, we also refer to the relevant Non-Provider Condition.

Table 1: An overview of requirements and to whom they apply

Requirement	This requirement applies to:	Providers are required to:
P2P mobile messaging		
Setting volume limits for pay-as-you-go (PAYG) SIMs (including eSIMs)	Mobile operators that transfer and/or terminate P2P messages.	Set volume limits for PAYG SIMs to make it harder for scammers to message large numbers of potential victims (GCs C9.4 and C9.5).
Receiving scam reports relating to their customers	Mobile operators that have assigned mobile numbers.	Have processes to regularly and proactively ensure they receive scam reports, from customers and from appropriate third parties, relating to the customers they have assigned mobile numbers to (GC C9.2(a)).
Receiving other scam reports	Mobile operators that transfer and/or terminate P2P messages.	Have processes to regularly and proactively ensure they receive scam reports, from customers and from appropriate third parties, relating to telephone numbers and URLs that have been used for scams (GCs C9.2(b) and (c)).
Blocking numbers used by scammers	Mobile operators that have assigned mobile numbers.	Prevent scammers from sending messages from numbers that they believe have sent scam messages, based on information from scam reports (GC C9.3(a)).
Blocking scam messages in transit	Mobile operators that transfer and/or terminate P2P messages.	Identify and block scam messages that originate from telephone numbers that providers believe have been used for scams; or that contain URLs and telephone numbers that providers believe have been used for scams, based on information from scam reports (GCs C9.3(b) and C9.3(c)).

[9] United Nations Human Rights Office of the High Commissioner. Guiding Principles on Business and Human Rights.

[10] While this table provides a high-level overview, further detail on to which entities each obligation applies is set out in the guidance for each requirement.

Requirement	This requirement applies to:	Providers are required to:
A2P mobile messaging		
Receiving scam reports	Mobile operators and tier 1 aggregators that transfer and/or terminate A2P messages.	Have processes to regularly and proactively ensure they receive scam reports, from customers and from appropriate third parties, relating to telephone numbers and URLs that have been used for scams (GC C9.6 and Non-Provider Condition 3.2).
Blocking scam messages in transit	Mobile operators and tier 1 aggregators that transfer and/or terminate A2P messages.	Identify and block scam messages that contain URLs and telephone numbers that providers believe have been used for scams, based on information from scam reports (GC C9.7 and Non-Provider Condition 3.3).
Conducting due diligence	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Ensure that Know Your Customer (KYC) checks take place on their traffic, to verify who new business senders are and assess their risk of sending scam messages (GCs C9.8, C9.9, C9.10 and C9.14 and Non-Provider Conditions 3.4, 3.5, 3.6 and 3.10).
	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Prevent the use of fake alphanumeric sender IDs (GCs C9.8, C9.9, and C9.11 and Non-Provider Conditions 3.4, 3.5 and 3.7).
	Mobile operators that terminate A2P messages.	Have policies on protected IDs, generic IDs and special alphanumeric characters (GC C9.13 and Non-Provider Condition 3.9).
Requirements for ongoing checks	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Carry out Know Your Traffic (KYT) checks to monitor a range of scam indicators and ensure scammers cannot use A2P channels to send scam messages (GCs C9.8, C9.9 and C9.12 and Non-Provider Conditions 3.4, 3.5 and 3.8).
Contractual requirements	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Set clear and unambiguous terms for the party from which they receive the A2P messages to either: undertake the KYC, alphanumeric Sender ID and KYT checks; or ensure that these checks have been conducted by a party in the downstream chain. (GC C9.9 and Non-Provider Condition 3.5).

Requirement	This requirement applies to:	Providers are required to:
Incident management requirements	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Quickly identify business senders that send scam messages and take appropriate measures to prevent them sending further messages (GCs C9.15 and C9.16 and Non-Provider Conditions 3.11 and 3.12).

Requirement	This requirement applies to:	Providers are required to:
Cross-cutting measures		
Right to challenge	In the context of P2P messages, mobile operators that transfer and/or terminate P2P messages and/or have assigned mobile numbers. In the context of A2P messages, mobile operators and tier 1 aggregators that transfer and/or terminate A2P messages. These are providers that carry out blocking under GC C9.3 and C9.7.	Implement and maintain appropriate and effective policies, systems and processes that enable any affected person to challenge any blocking of a message or number under GC C9.3 or C9.7 (GC C9.17 and Non-Provider Condition 3.13 but in relation to Condition 3.3). Requires an accessible and reasonably prominent policy explaining the right to challenge, including on providers' websites (GC C9.18 and Non-Provider Condition 3.14).
Review of policies, systems and processes	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers.	Regularly review their policies, systems and processes implemented under GC C9 to confirm that they remain appropriate and effective and are operating as intended (GC C9.19 and Non-Provider Condition 3.15 in relation to Condition 3).
Training staff	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers.	Ensure that all relevant staff are trained on the policies, systems and processes in place under Condition C9, including on the right to challenge processes (GC C9.20 and Non-Provider Condition 3.16).
Record keeping	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers, as applicable. Providers will only need to comply with a subset of the requirements as relevant to their business.	Implement and maintain appropriate record keeping policies, systems and processes (GCs C9.21-C9.25 and Non-Provider Conditions 3.17-3.21).

Requirement	This requirement applies to:	Providers are required to:
Identifying, monitoring and addressing false positives	Mobile operators and tier 1 aggregators that transfer and/or terminate P2P or A2P messages, as applicable. Providers that carry out blocking under GC C9.3(b) and (c) and C9.7 will need to comply.	Implement and maintain appropriate and effective policies, systems and processes to identify and monitor false positives under GCs C9.3(b) and (c) and C9.7 and take appropriate action when these are identified (GC C9.26 and Non-Provider Condition 3.22 in relation to Condition 3.3).
Data protection	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages, and/or that have assigned mobile numbers.	Ensure they comply with relevant data protection legislation when complying with GC C9 (GC C9.27 and Non-Provider Condition 3.23 in relation to Condition 3).

2. Guidance

Structure of this section

2.1 This section sets out guidance for providers to comply with protections for end-users from scam mobile messages under GC C.9. Where relevant, we also identify the corresponding rule in Non-Provider Condition 3.

2.2 With respect to P2P messaging, the guidance covers how providers may meet their obligations to:

- Have processes to regularly and proactively ensure they receive scam reports relating to telephone numbers they have assigned, other telephone numbers and URLs that are being used for scams, including on P2P channels (GC C9.2).
- Block suspicious numbers and messages (GC C9.3) and apply volume limits to Pay As You Go (PAYG) customers (GCs C9.4 and C9.5), to address P2P messaging scams.

2.3 With respect to A2P messaging, the guidance covers how providers may meet their obligations to:

- Have processes to regularly and proactively ensure they receive scam reports relating to telephone numbers and URLs that are being used for scams, including on A2P channels (GC C9.6).
- Block suspicious messages (GC C9.7) and implement robust due diligence, monitoring and incident management processes to prevent misuse of A2P services (GCs C9.8 to C9.16).

2.4 With respect to the cross-cutting measures, the guidance covers how providers may meet their obligations to:

- Implement and maintain a right to challenge (GC C9.17 and C9.18), keep operations under review (GC C9.19), train staff (GC C9.20), ensure good record keeping (GCs C9.21 to C9.25), identify, monitor and address false positives (GC C9.26) and comply with relevant data protection legislation (GC C9.27).

Guidance on rules to combat P2P scam mobile messages

2.5 Below, we describe how mobile operators can comply with the obligations under GCs C9.2 to C9.5 to combat P2P scam messages. The guidance covers how providers may meet their obligations with respect to P2P messaging, as relevant, to

- Receiving scam reports in relation to P2P messages (GC C9.2).
- Preventing P2P scam messages from being sent or received (GC C9.3).
- Setting volume limits for PAYG customers (GC C9.4 and GC C9.5).

Receiving scam reports in relation to P2P Messages

C9.2 Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) Scam Reports from End-Users and appropriate third parties, relation to:

(a) Customers they have assigned Mobile Numbers to;

(b) Telephone Numbers that the End-User and/or third party believes sent P2P Messages intended to Scam the recipients; and

(c) URLs and Telephone Numbers that the End-User and/or third party believes were used as part of a Scam, including URLs and Telephone Numbers included in P2P Messages.

Who this obligation applies to

2.6 GC C9.2(a) applies to any Communications Providers that have assigned mobile numbers, i.e. all mobile operators, including MNOs, thick MVNOs and thin MVNOs. GCs C9.2(b) and (c) apply to Communications Providers that transfer and/or terminate P2P Messages, i.e. mobile operators that are MNOs or thick MVNOs. [11] GCs C9.2(b) and (c) do not apply to thin MVNOs.

Purpose of receiving scam reports

2.7 The purpose of receiving scam reports is to strengthen mobile operators' ability to detect telephone numbers and messages associated with scams, based on intelligence relating to their customers, telephone numbers and URLs.

2.8 This requirement should support the targeted, intelligence-led blocking of scam numbers and messages, as set out at GC C9.3.

Sources and mechanisms for receiving scam reports

2.9 Mobile operators are required to implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) reports of scams from end-users and appropriate third parties on:

- Customers they have assigned Mobile Numbers to.
- Telephone Numbers (including Mobile Numbers) that have been reported as sending P2P messages intended to scam the recipients.
- URLs and Telephone Numbers that have been reported as being used as part of a scam, including URLs and Telephone Numbers included in P2P messages.

2.10 We require mobile operators (including thin MVNOs) to receive scam reports about numbers they have assigned to customers. This includes receiving direct complaints from the public or through third party scam reports such as those from the 7726 service (we expect thin MVNOs to obtain such 7726 scam reports from their host MNOs).

2.11 We expect mobile operators to implement adequate mechanisms to allow their own customers to report suspected scam messages: for example, by ensuring customers can:

- Easily forward, or use reporting functionality built into messaging applications, to report a suspected scam message to their own provider or to a reliable third party that will take responsibility for collating scam messages and providing the collected intelligence back to the customer's provider (such as the 7726 service); and/or
- Access an internet web page form or email account that is regularly checked and allows them to report a suspected scam message.

2.12 We also expect mobile operators to offer advice to their customers on how they can report suspected scams if they receive them. They can do this by publishing information on web

[11] See GC C9.1 for the exact scope of the obligation.

pages for customers (e.g. Q&As) and/or ensuring that customer service operatives are trained to provide appropriate advice on how to report messaging scams. Mobile operators should make clear to their customers that they may block messages on the basis of customers' reports, taking into account data protection principles including fairness and transparency.

2.13 To comply with GC C9.2, we do not consider that it would be sufficient for mobile providers to enable their own customers to report scams, only. Mobile operators should establish and maintain processes to obtain reports from a range of sources, including from appropriate third parties. Obtaining intelligence from a range of sources will enable mobile operators to act on scam reports that customers of other mobile operators have generated. Reports should also contain information on scams received via channels other than P2P messages (e.g. A2P messages).

2.14 When deciding which third parties are appropriate to rely on for scam reports, mobile operators are expected to take into account the extent to which those third parties have expertise in and a legitimate basis for identifying or aggregating scams, provide a rich source of timely information and can provide detailed information on current and emerging threats. In doing so, the use of appropriate third parties is intended to protect the integrity and efficacy of reporting systems.

2.15 Appropriate third parties could include (but are not limited to):

- Consumer reports included in the 7726 database, which include scam reports from multiple mobile operators.
- Cyber Defence Alliance data, which contains information on scam URLs.
- The National Cyber Security Centre's Share and Defend capability.
- Global Signal Exchange.
- Cifas services (such as its National Fraud Database).
- TUFF (Telecommunications UK Fraud Forum).
- Stop Scams UK.

2.16 It is for mobile operators to identify which sources best help them meet their regulatory obligations and to seek to arrange access to these sources. The inclusion of examples of sources of scam reports, above, does not imply that mobile operators will have the right to access these sources. Providers may also wish to obtain intelligence on scams from other appropriate third parties, such as law enforcement and financial services institutions or other organisations identified by UK Government[12] or other regulators.

Tailoring scam report requirements to a mobile operator's identifying and blocking capabilities

2.17 The type and extent of the scam reports that is appropriate for mobile operators to gather may depend on what kind of provider they are. For example, thin MVNOs that rely on an MNO to block messages in transit will not need to obtain intelligence relating to scam URLs and telephone numbers included in the content of a message. They are only required to ensure they receive information under GC C9.2(a), on telephone numbers suspected of

[12] Providers may also want to consider obtaining scam intelligence from organisations that have been designated as Specified Anti-Fraud Organisations (SAFOs) under section 68 of the Serious Crime Act 2007.

sending scam messages. They could use this data to cross refer against their own customers and, if appropriate, implement a block as required under GC C9.3(a).

Scrutiny and validation of scam reports

2.18 When using scam reports for the purpose of preventing numbers from sending messages or for blocking messages (under the requirements of GC C9.3, explained below), mobile operators must have reasonable grounds to believe that numbers or messages identified in scam reports were intended to scam the intended recipients.

2.19 Mobile operators should therefore take appropriate steps to mitigate the risk of legitimate numbers or messages in scam reports (false positives), including by validating scam reports (where appropriate).

2.20 Mobile operators should recognise that scam reports (including from third-party intelligence) may contain incorrectly classified or benign messages and undertake an appropriate level of validation of the information included in scam reports.

2.21 Certain sources of scam reports (such as lists of known scam URLs provided by a credible third party) may not require significant scrutiny if the third party has already undertaken this step.

2.22 Where providers consider it appropriate to validate scam reports, we expect them to interrogate scam reports to filter out messages that they do not reasonably believe were intended to scam the recipients. When doing so, mobile operators are expected to consider taking the following steps:

- Regularly obtaining scam reports that are current and robust, ideally gathered through automated systems that are regularly updated to reflect real-time developments in scam tactics.
- Using contextual testing and evaluation (which may include human review) to verify whether information in scam reports appears accurate and complete and refining the data before using it to inform blocking decisions.
- Assessing the context in which a message was sent (for example, checking whether messages purporting to be from trusted organisations were sent as P2P messages) and verifying URLs against known domains.
- Interrogating whether a number reported as malicious may belong to a legitimate user whose number has been spoofed[13] or whether reports may have flagged legitimate numbers that were sent using a spoofed alphanumeric Sender ID.[14]
- Considering whether and how it may be possible to identify messages where an individual may copy a scam URL or telephone number to send to a friend, to warn them about a scam.[15]
- Using multiple intelligence inputs, where appropriate, including internal data and trusted external datasets.

[13] In a P2P channel, a scammer may spoof a legitimate mobile number that recipients may report, leading to that legitimate number being categorised as malicious.
[14] In an A2P channel, a scammer may use a spoofed Alphanumeric Sender ID (e.g. a bank's name), meaning reports associated with the message may wrongly identify a legitimate Alphanumeric Sender ID as malicious.
[15] In this case, while the individual's message may be blocked, it should mean an actual scam message containing the relevant URL or telephone number is also blocked, mitigating the risk that the intended recipient will be harmed by the relevant message.

- Feeding learnings from challenges and false positives that they identify back into validation checks.
- Considering what steps they can take to mitigate the risk of an error occurring in the provider's systems and processes: for example, in the way they obtain, validate and subsequently use scam reports as an input to blocking tools, or in an underlying database for processing scam reports.

2.23 Providers may also wish to consider the extent to which scam reports identify malicious URLs or Sender IDs in Welsh and whether their identifying and blocking measures may be able to identify and block numbers and messages sent from, or that contain, those malicious URLs or Sender IDs.

2.24 Robust validation of scam reports will help ensure compliance with the data accuracy principle under the UK General Data Protection Regulation 2016 (UK GDPR).

2.25 Mobile operators are expected to use messages as a source of intelligence to inform scam reports only where a user has reported it (e.g. to 7726) and consented (explicitly or implicitly) to review of their message, on the basis that it is a potential scam.

Sharing scam reports with other providers and third parties

2.26 We encourage mobile operators to establish intelligence-sharing mechanisms to disrupt scam messages and prevent these from reaching consumers. We expect operators to collect intelligence of scam activity from a broad range of sources, which includes scam reports and other measures related to GC C9, for example reports of Significant Scams Incidents.[16] Sharing data they hold with other mobile operators and third parties will help strengthen the quality, timeliness and comprehensiveness of the intelligence available to all providers.

2.27 Examples of how operators could share scam reports include:

- Contributing to shared industry databases or alerting platforms where scam indicators such as Sender IDs, URLs and telephone numbers associated with scams are circulated in real time.
- Consolidating and sharing scam intelligence submitted through reporting services (such as 7726) with other providers to identify campaigns affecting multiple networks.

2.28 When establishing intelligence-sharing mechanisms to share scam reports and other intelligence, providers should consider what safeguards would be appropriate to put in place to ensure compliance with relevant data protection legislation and competition law. Examples of such safeguards include:

- Taking into account any guidance issued by Government and/or the Information Commissioner's Office (ICO) (as amended from time to time) on how to comply with relevant data protection legislation[17] when sharing personal data relating to fraud and scams.[18]
- Where possible, anonymising, aggregating or removing any personal data.

---

[16] A 'Significant Scams Incident' is defined in our GCs as a situation where it appears to a provider that a particular business sender has cumulatively sent or attempted to send, directly or indirectly, at least fifty A2P messages that the provider reasonably believes were intended to scam the recipients.

[17] Relevant data protection legislation is discussed in paragraphs 2.248-2.260 below.

[18] See, for example, ICO, Sharing personal information when preventing, detecting and investigating scams and frauds [accessed on 8 July 2026].

- Sharing the minimum amount of information necessary for the specific purpose of significantly reducing the likelihood that consumers receive scam messages.
- Restricting access to information both internally and externally: for example, by implementing confidentiality safeguards and/or data sharing agreements to ringfence any information that is provided and ensure it is only provided to authorised individuals, on a strictly need-to-know basis, for the specific purpose for which it has been provided.
- Providers keeping a brief record of what they share, with whom, why, and the expected outcome (as well as any confidentiality or data sharing agreements they implement).

2.29 We note that data protection law is not a barrier to sharing data for fraud prevention but is a framework for doing so responsibly. The UK GDPR and the Data Protection Act 2018 both contain specific provisions that support the sharing of personal data to prevent and detect crime, including fraud. The Data Use and Access Act 2025 further strengthened these foundations by amending the UK GDPR to introduce a new "recognised legitimate interests" basis for processing, which includes fraud prevention.[19] The ICO's guidance on sharing personal information when preventing, detecting and investigating scams and fraud states that:

> *"Effective data sharing between organisations and across different digital sectors is an important factor in preventing data-enabled scams and fraud.*
>
> *The UK GDPR and the Data Protection Act 2018 (DPA) do not prevent you from sharing personal information where it is appropriate to do so, or from taking steps to prevent harm."*[20]

Preventing P2P scam messages from being sent or received

> **C9.3** Taking into account Scam Reports received, Regulated Providers must implement and maintain appropriate and effective policies, systems and processes designed to:
>
> (a) prevent, without undue delay, Mobile Numbers they have assigned to a Customer from sending P2P Messages where they reasonably believe those Mobile Numbers have sent P2P Messages intended to Scam the intended recipients;
> (b) block, without undue delay, P2P Messages sent from Telephone Numbers where they reasonably believe those Telephone Numbers to have sent P2P Messages intended to Scam the intended recipients; and
> (c) block, via automated means and without undue delay, P2P Messages that contain URLs or Telephone Numbers which they reasonably believe were used as part of a Scam.

Who this obligation applies to

2.30 GC C9.3(a) applies to any Communications Providers that have assigned mobile numbers, i.e. all mobile operators, including MNOs, thick MVNOs and thin MVNOs. GCs C9.3(b) and (c) apply to Communications Providers that transfer and/or terminate P2P Messages, i.e.

[19] See, Article (ea) and paragraph 5(a) of Annex 1 of the UK GDPR.
[20] See ICO, Sharing personal information when preventing, detecting and investigating scams and frauds [accessed on 8 July 2026].

mobile operators that are MNOs or thick MVNOs that have their own SMSC.[21] GCs C9.3(b) and (c) do not apply to thin MVNOs that do not have their own SMSC and rely on their host MNO to transfer and terminate messages.

Purpose of scam blocking measures

2.31 The purpose of these measures is to ensure a more consistent and effective approach to number and message blocking across the mobile sector. These requirements set out that numbers should be blocked from sending messages, and messages should be blocked in transit, where it is reasonable to believe that they are being used/sent by scammers.

Blocking numbers used by scammers

2.32 Taking into account scam reports received (including in accordance with GC C9.2 and, where applicable, GC C9.6), mobile operators must implement and maintain appropriate and effective policies, systems and processes designed to prevent, without undue delay, mobile numbers they have assigned to a customer from sending P2P messages where they reasonably believe those mobile numbers have sent P2P messages intended to scam the intended recipients.

2.33 We expect all mobile operators (including thin MVNOs) that have assigned mobile numbers can comply with this obligation by feeding validated scam report information into fraud prevention systems to identify customers' mobile numbers that are suspected of sending scams and take appropriate steps to block them from sending further messages. As such providers will hold a direct contractual relationship with the customer using the mobile number, we expect that they should be able to investigate the circumstances surrounding its use and have the technical capability to block that customer's number from sending further messages.

2.34 For the avoidance of doubt, this rule does not require mobile operators to review the content of messages that a number has sent before deciding to block that number.

Identifying and blocking scam messages in transit

2.35 Taking into account scam reports received (including in accordance with GC C9.2 and, where applicable GC C9.6), mobile operators must implement and maintain appropriate and effective policies, systems and processes designed to:

- Block, without undue delay, P2P messages sent from telephone numbers where they reasonably believe those telephone numbers to have sent P2P messages intended to scam the intended recipients.
- Block, via automated means and without undue delay, P2P messages that contain URLs or telephone numbers which they reasonably believe were used as part of a scam.

2.36 MNOs are responsible for identifying and blocking scam messages in transit on their network. This includes messages sent to or from their thin MVNO partner's customers and we expect MNOs and their thin MVNO partners to have arrangements in place under which the MNO agrees to carry out blocking on their behalf.

2.37 The obligation in GC C9.3(b) allows the use of automated tools or human review and does not require mobile operators to review the content of messages.

[21] See GC C9.1 for the exact scope of the obligation.

2.38 The obligation in GC C9.3(c) requires mobile operators to use automated tools to examine specific message content (i.e. any URLs or telephone numbers that messages contain), where necessary. Providers may adopt different tools to comply: for example, providers may decide to input rules into their scam prevention systems or adopt tools that compare the content of messages against a database.

2.39 Mobile operators are expected to consider whether they can use other indicators of malicious activity to block messages before reviewing message contents. For example, where a source Sender ID or Global Title[22] is present in an internal blocklist, these should be used to block the message, before it may be necessary to examine the message's content. They can achieve this by ordering the application of firewall systems rules to examine message contents last.

2.40 Mobile operators could consider applying quarantine functionality to temporarily hold messages that cannot be confidently classified as legitimate or illegitimate. This allows time for further traffic analysis and supports more accurate blocking decisions. Mobile operators should also consider if there are specific scenarios where a legitimate message may contain a scam URL or telephone number (see paragraph 2.22 above) and take appropriate steps to ensure that the end-user's number is not blocked.

2.41 We recognise that some degree of human review of messages is likely to be necessary to ensure automated tools are working as intended. This is not prohibited by our rules.

2.42 Mobile operators will need to comply with relevant data protection legislation (see paragraphs 2.248-2.260, below).

Managing the risk of false positives

2.43 One way in which false positives may arise is as a result of system of human errors (for example, where a rule is incorrectly inputted into a provider's scam prevention system or where blocking tools are not working as intended).

2.44 When designing and implementing blocking measures, providers should therefore take appropriate steps to minimise the risk of incorrectly blocking legitimate messages. This should include:

- Testing and validating blocking rules prior to deployment, including by assessing whether rules or thresholds may inadvertently capture legitimate traffic.
- Ensuring appropriate human oversight and governance processes, particularly where new rules or changes to existing rules are introduced (for example, by ensuring all or certain rules or changes that may have a significant impact are peer reviewed and signed off by senior responsible individuals).
- Monitoring the impact of blocking measures following implementation, including reviewing whether the blocking is working as intended (under GC C9.19) and taking appropriate, effective and prompt action when they identify false positives to mitigate the risk of further false positives arising under GC C9.26 (for example, by amending rules in their scam prevention systems).

[22] Global Titles are numbers created from ranges of mobile numbers we allocate to mobile operators. Mobile operators use Global Titles as a routing address for the exchange of signalling messages with other operators and to support their provision of mobile services.

2.45 The measures above should help minimise the risk of incorrectly blocking legitimate messages. However, false positives cannot be eliminated entirely, and providers should therefore implement and maintain appropriate arrangements to identify, monitor and address false positives, as required by GC C9.26.

2.46 Further guidance is set out at paragraphs 2.229-2.245

Setting volume limits for Pay As You Go customers

C9.4 Regulated Providers must implement and maintain appropriate and effective policies, systems and processes setting limits on the volume of P2P Messages that their Pay As You Go Customers can send from a specific Mobile Number, in a specified period, to any Mobile Number, with the objective of preventing Scam messages from being sent and/or received.

C9.5 Regulated Providers must block, via automated means and without delay, Pay As You Go Customers from sending any further P2P Messages where that Pay As You Go Customer reaches any volume limit imposed by the Regulated Provider in line with the policy it has implemented under Condition C9.4, for the duration of the time specified in the policy.

Who this obligation applies to

2.47 GCs C9.4 and C9.5 apply to Communications Providers that transfer and/or terminate P2P Messages,[23] i.e. mobile operators that are MNOs and thick MVNOs.

The purpose of volume limit measures

2.48 The use of volume limits is intended to disrupt messaging scams by preventing scammers from sending large volumes of messages quickly and easily. By making bulk messaging via Pay As You Go (PAYG) SIMs more difficult and costly, these limits aim to reduce the number of scam mobile messages reaching end-users.

Setting a policy on volume limits

2.49 For the purposes of GC C9, PAYG customers, also known as pre-pay customers, include any customer that has accessed a mobile service without being on a fixed post-pay contract. This includes no-contract monthly rolling options, where the customer pays a recurring fee in advance for a service, traditional top-up-based SIMs and any hybrid of the two. In other words, it includes any customer that requires a pre-pay credit balance to continue to use the mobile service, or services outside of any inclusive allowance. PAYG customers also include customers that access mobile services either directly from an MNO or thick MVNO or indirectly via a thin MVNO that uses a host mobile operator's network. Further, the obligation to apply volume limits applies to PAYG customers using any type of SIM, including SIMs made available or obtained electronically (eSIMs).[24]

2.50 Under this requirement, a mobile operator may determine the details of its own volume limit policy. The policy may also differ depending on the particular product or service. Our obligation falls on MNOs and thick MVNOs that use their own SMSC to transfer and terminate P2P messages (see paragraph 1.11). We understand that some thin MVNOs may be able to implement an effective volume limit through their billing systems, for example.

[23] See GC C9.1 for the precise scope of the obligation.
[24] See the definition of 'Pay As You Go Customer' in the GCs.

However, there may be a significant delay in applying a limit where communication between a host MNO and a thin MVNO is required, which may undermine the effectiveness of the limit. Therefore, the obligation falls on MNOs to ensure compliance with GCs C9.4 and C9.5 in relation to SIMs distributed by their thin MVNOs partners (or branded resellers) and MNOs will be responsible for ensuring that thin MVNO (or branded reseller) partners comply with our volume limits measure.

2.51 MNOs should therefore work with their thin MVNO partners to discuss and agree specific terms for implementing and maintaining an appropriate and effective policy on volume limits. For example:

- The MNO may expect its thin MVNO partners to agree to a default volume limit or the same volume limit the MNO applies to its own customers; or
- The MNO may agree to apply a different volume limit to its thin MVNO's customers where justified by traffic patterns associated with that thin MVNO's customers.

2.52 We provide examples in paragraph 2.61 of how MNOs can ensure a SIM is blocked when a volume limit has been reached by one of its thin MVNO partners.

2.53 In considering what volume limit may be appropriate in any given circumstance, we would expect mobile operators to take into account:

- The volume and frequency of messages that a scammer might be expected to send.
- Whether it is likely to be more effective to impose strong limits for an initial period after a SIM is first used for messaging, if past trends suggest that scammers tend to send most of their messages shortly after a SIM is first acquired or activated.
- Typical use by legitimate users on the mobile operator's network, taking into account the type of customers the provider has and past usage patterns.
- Whether there are legitimate high-volume business messages that might be able to use A2P channels (which would be subject to further due diligence and monitoring measures), rather than increasing a P2P volume limit to allow for those types of messages.
- Whether hourly, daily, weekly or monthly volume limits are the most appropriate.
- Whether it is necessary to reset limits, given that legitimate senders will know when a volume limit has been applied and their SIM has been blocked and could potentially restore their service by contacting their provider.

2.54 When considering the factors above, mobile operators may wish to consider industry-wide scams intelligence, as well as its own intelligence based on scams identified on its network.

2.55 Where technically feasible, we recommend that mobile operators monitor the number of unique recipient numbers a customer has sent messages to and incorporate this into their volume limit policy. Sending messages to a large number of recipients within a small time period is more likely to indicate scam activity than where there is only one, or a small number of recipients. Considering the number of unique recipients may therefore aid the detection of fraudulent activity and help to avoid penalising legitimate users.

2.56 Once mobile operators have decided on an appropriate volume limit policy, they must record that limit in an internal policy. We discuss record keeping further below at paragraphs 2.208-2.212.

2.57 To ensure volume limits remain effective and do not interfere with legitimate use, mobile operators should have a volume limit policy that is flexible and risk based. We also expect mobile operators to regularly review and assess the impact of their volume limits. This includes keeping any policy under which a volume limit is reset (allowing the end-user to send messages again) under close review and revising it if it becomes clear that setting the caps in such a way is not effective in preventing scammers from sending messages at scale. We discuss obligations relating to the review of anti-scam measures further below at paragraphs 2.187-2.196.

Implementing a block when the limit has been reached

2.58 Mobile operators must block, via automated means and without delay, PAYG customers from sending any further P2P messages where that customer reaches any volume limit imposed by the mobile operator in line with the policy it has implemented under GC C9.4, for the duration of the time specified in the policy.

2.59 We expect the block to be implemented instantaneously or as soon as possible after the volume limit has been reached, taking into account that any delay has the potential to significantly undermine the effectiveness of the volume limit and increase the risk that scam messages reach consumers.

2.60 As noted above, MNOs are responsible for compliance with GC C9.5 in relation to their thin MVNO partners. However, it is for MNOs to work with their MVNO partners to determine the necessary arrangements to ensure a SIM is blocked via automated means and without delay after a limit is reached.

2.61 Examples of how this may be done include:

- The thin MVNO using their own fraud prevention system, such as a billing system, to implement an agreed volume limit if it would satisfy our 'without delay' requirement. In this case, we would expect the MNO to offer effective system support to the thin MVNO if needed.
- The MNO implementing an agreed volume limit on behalf of the thin MVNO by blocking the SIM of the MVNO's customers that have reached the limit.

2.62 We expect mobile operators to send a message to the SIM that has been blocked, explaining that the limit has been reached and will not be able to send further messages.

Guidance on rules to combat A2P scam messages

2.63 This sub-section describes how providers (including mobile operators, aggregators and other persons that have been allocated numbers[25] and fall in scope of the Non-Provider Conditions) can comply with the A2P requirements under GC C9 and Non-Provider Condition 3, as applicable. The guidance focuses on the GCs, although we have noted the corresponding Non-Provider Conditions in a footnote where relevant.

2.64 The guidance covers how providers may meet their obligations with respect to A2P messaging, as relevant, to:

- Receive scam reports in relation to A2P messages (GC C9.6).
- Prevent A2P scam messages from being sent or received (GC C9.7).

[25] Including sub-allocations.

- Ensure due diligence and on-going checks are conducted, (GC C9.8), including:
  - Know Your Customer (KYC) checks (GC C9.10).
  - Checks on the use of new alphanumeric Sender IDs (GC C9.11).
  - Know Your Traffic (KYT) checks (GC C9.12).
  - Contractual requirements (GC C9.9).
- Set a policy on protected alphanumeric Sender IDs (GC C9.13).
- Require notification of changes to business profiles (GC C9.14).
- Implement incident management requirements (GCs C9.15-C9.16).

Receiving scam reports in relation to A2P messages

C9.6[26] Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) Scam Reports from End-Users and appropriate third parties in relation to URLs and Telephone Numbers that the End-User and/or third party believes were used as part of a Scam, including URLs and Telephone Numbers included in A2P Messages.

Who this obligation applies to

2.65 GC C9.6 applies to any Communications Provider that transfers and/or terminates A2P Messages, except a Lower-Tier Aggregator.[27] GC C9.6 applies to mobile operators that enable A2P termination to their customers (including MNOs and some thick MVNOs) and tier 1 aggregators. This obligation does not apply to (a) MVNOs that do not have their own SMSC and/or rely on their host MNO to transfer and terminate A2P Messages; or (b) lower-tier aggregators that do not contract directly with the mobile operator that terminates the messages to recipients.

Purpose of receiving scam reports

2.66 The purpose of having processes to receive scam reports is to strengthen the ability of mobile operators and tier 1 aggregators to detect and block scam messages from reaching end-users, based on intelligence relating to URLs and telephone numbers.

Sources and mechanisms for receiving scam reports

2.67 The guidance we have set out at paragraphs 2.9 to 2.29 on how providers can meet their obligations under GC C9.2 is also applicable to A2P messages.

2.68 Providers are expected to obtain intelligence on scams from a range of sources that is not limited to scams that may have arisen in A2P messages. They are also expected to source scam reports that have been generated from customers of other providers and appropriate third parties. In paragraphs 2.15-2.16, we have set out guidance on what would be appropriates source of scams intelligence, which is also applicable to A2P messages. These sources could include (but are not limited to):

[26] Non-Provider Condition 3.2 corresponds to GC C9.6.
[27] See Condition 3.1(a) for the scope of the corresponding Non-Provider Condition (Condition 3.2).

- Consumer reports included in the 7726 database, which include scam reports from multiple mobile operators.
- Cyber Defence Alliance data, which contains information on scam URLs.
- The National Cyber Security Centre's Share and Defend capability.
- Global Signal Exchange.
- Cifas services (such as its National Fraud Database).
- TUFF (Telecommunications UK Fraud Forum).
- Stop Scams UK.

2.69 It is for mobile operators and tier 1 aggregators to identify which sources best help them meet their regulatory obligations and to seek to arrange access to these sources. The inclusion of examples above does not in any way give providers an automatic right to access these sources.

2.70 Providers may also wish to obtain intelligence on scams from other appropriate third parties, such as law enforcement and financial services institutions or other organisations identified by UK Government[28] or other regulators.

2.71 In addition, we would expect tier 1 aggregators to have arrangements in place with terminating providers to receive intelligence from terminating mobile operators.

Scrutiny and validation of scam reports

2.72 Providers must have a reasonable belief the numbers or messages identified in scam reports were intended to scam the intended recipients when using information for the purposes of GC C9.7. Providers should therefore undertake an appropriate level of validation of the information included in the scam reports.

2.73 The guidance above at paragraphs 2.18 to 2.25 on scrutiny and validation of scam reports also applies here.

Sharing scam reports with other providers and third parties

2.74 As explained in paragraph 2.26 above, providers are encouraged to establish intelligence-sharing mechanisms to disrupt scam mobile messages and prevent them from reaching consumers. As set out above, sharing data they hold with other mobile operators and third parties will help strengthen the quality, timeliness and comprehensiveness of the intelligence available to all providers. We expect operators to collect intelligence of scam activity from a broad range of sources, which includes scam reports and other measures related to condition C9, for example reports of Significant Scams Incidents. Sharing data helps each provider build a more robust and up to date understanding of scam activity. When providers rely solely on reports from their own customers, they risk working with an incomplete picture. By contrast, pooling reports from customers of multiple providers creates a more comprehensive and accurate dataset.

2.75 We therefore encourage mobile operators and tier 1 aggregators to establish intelligence-sharing mechanisms for the purpose of significantly reducing the likelihood that consumers receive scam messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law. Examples of such safeguards are set out at paragraph 2.28, above.

[28] Providers may also want to consider obtaining scam intelligence from organisations that have been designated as Specified Anti-Fraud Organisations (SAFOs) under section 68 of the Serious Crime Act 2007.

2.76 The guidance above at paragraphs 2.26 to 2.29 on sharing scam reports with other providers and third parties also applies here.

Preventing A2P scam messages from being sent or received

> **C9.7**[29] Taking into account Scam Reports received, Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to block, via automated means and without undue delay, A2P Messages that contain URLs or Telephone Numbers which they reasonably believe were used as part of a Scam.

Who this obligation applies to

2.77 GC C9.7 applies to any Communications Provider that transfers and/or terminates A2P Messages, except Lower-Tier Aggregators.[30] GC C9.7 applies to mobile operators that enable A2P termination to their customers (including MNOs and some thick MVNOs) and tier 1 aggregators. This obligation does not apply to (a) MVNOs that do not have their own SMSC and/or rely on their host MNO to transfer and terminate A2P Messages; or (b) lower-tier aggregators that do not contract directly with the mobile operator that terminates the messages to recipients.

Purpose of this requirement

2.78 The purpose of this measure is to ensure a more consistent and effective approach to message blocking across the sector. We expect providers to detect and block messages already in transit that contain telephone numbers or URLs they reasonably believe have been used to facilitate scams.

Identifying and blocking scam messages in transit

2.79 Taking into account the scam reports they have received (including in accordance with GC C9.6 and, where applicable, GC C9.2), providers must implement and maintain appropriate and effective policies, systems and processes to block, via automated means and without undue delay, A2P messages that contain URLs or Telephone Numbers that they reasonably believe were used as part of a scam.

2.80 The guidance set out at paragraphs 2.35 to 2.42, on how providers can meet the equivalent obligations in GC C9.3 in relation to P2P messages, is also applicable here.

2.81 In specific circumstances, an appropriate and effective policy may allow for A2P messages from a limited number of business senders to not be subject to a provider's general identifying and blocking measures that it would apply to other A2P messages, provided certain conditions are met. This may be appropriate where, at a minimum:

- The provider has a direct and robustly verified relationship with a major business sender that it has established has a very low risk of fraud or has robustly verified that such a business sender has given permission for specified aggregators to use its alphanumeric Sender ID exclusively.
- The provider keeps appropriate records explaining why it considers it appropriate to take this approach for a specific business sender and why it considers its approach remains effective at blocking messages with scam URLs or telephone numbers.

[29] Non-Provider Condition 3.3 corresponds to GC C9.7.
[30] See Condition 3.1(a) for the scope of the corresponding Non-Provider Condition (Condition 3.3).

- The provider keeps this process under regular review, including by monitoring scam reports and carrying out KYT checks for any scam indicators.

2.82 MNOs are responsible for identifying and blocking scam A2P messages in transit on their network. This includes A2P messages sent to their MVNO partners' customers, unless an MVNO partner manages and terminates A2P messages to their customers themselves. We expect MNOs and their MVNO partners to have arrangements in place under which the MNO agrees to carry out blocking on their behalf where applicable.

Due diligence and on-going checks

C9.8[31] Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to ensure that:

(a) for any A2P Messages that they transfer and/or terminate, Know Your Customer Checks, checks relating to the use of any Alphanumeric Sender IDs and on-going Know Your Traffic Checks are conducted in accordance with Conditions C9.10 to C9.12, either by the Regulated Provider:

(i) carrying out these checks themselves; or

(ii) taking the steps in Condition C9.9; and

(b) they do not transfer and/or terminate A2P Messages or enable the use of the relevant Alphanumeric Sender IDs unless they are reasonably satisfied with the outcome of these checks or with the checks carried out under Condition C9.9(a).

Who these obligations apply to

2.83 GCs C9.8 to C9.12 apply to any Communications Provider that transfers and/or terminates A2P Messages, including all Aggregators.[32] These GCs apply to mobile operators (including MNOs and some thick MVNOs) and all aggregators (whether they are acting at tier 1 or at lower tiers). These GCs do not apply to MVNOs that do not have their own SMSC and/or rely on their host MNO to transfer and terminate A2P Messages.

Purpose of these requirements

2.84 These requirements are intended to ensure that providers carry out appropriate checks on A2P business senders and message traffic and that messages are prevented from being transferred and/or terminated if these checks have not been satisfactorily carried out by the provider or a person in their downstream chain.

2.85 Different parties in the chain of providers involved in the delivery of A2P messages can take different actions to ensure these checks take place. The requirements recognise this by allowing providers to either carry out the required checks themselves or to satisfy themselves that they have been done via clear and unambiguous contractual terms with any party from which they receive messages.

[31] Non-Provider Condition 3.4 corresponds to GC C9.8.
[32] See Condition 3.1(b) for the scope of the corresponding Non-Provider Conditions (Condition 3.4-3.8).

Know Your Customer (KYC) checks

C9.10[33] Know Your Customer Checks must include:

(a) due diligence checks against Business Profiles for any indication that the Business Sender poses a risk of sending Scam messages;

(b) assessing the proposed use of any Alphanumeric Sender IDs for any indication that the Business Sender poses a risk of sending Scam messages, where applicable taking into account policies in place under Condition C9.13;

(c) confirmation of the contact details of a senior individual that is responsible for authorising the messages to be sent or transferred and/or terminated; and

(d) carrying out appropriate risk assessments to identify whether enhanced checks are appropriate to any cases, and if so, carrying out such checks.

Purpose of this requirement

2.86 The purpose of this requirement is to reduce the risk of scam messages entering the A2P supply chains by ensuring providers undertake appropriate due diligence before agreeing to convey A2P messages. The requirement establishes minimum standards for identifying business senders, assessing their risk profile, understanding the intended use of messaging services and carrying out enhanced checks where they find indicators of a risk of scams. Providers remain free to carry out more extensive checks where they consider this appropriate.

KYC checks

2.87 As part of assessing the risk that new business senders pose, providers will need to know on whose behalf they are agreeing to convey messages. When onboarding new business senders directly, GC C9.8(a) requires providers to perform KYC checks. Where providers are not onboarding the business sender directly, they are required to take steps (set out at GC C9.9) to ensure that the downstream party that is onboarding the business sender conducts equivalent checks.

2.88 If, instead of directly onboarding a new business sender, the provider receives A2P messages from another party, such as an aggregator or an MSP, they must agree clear and unambiguous contractual terms with that party to ensure that equivalent checks take place (see paragraph 2.89).

2.89 As part of these checks, we require providers to collect and assess a range of information to inform a documented risk assessment on whether the business sender poses a risk of sending scam messages. At a minimum, providers need to collect and assess the following information:

- Trading or registered names.
- Registered office or trading address.
- The nature of the service the business or organisation provides.
- Payment / bank account information.

[33] Non-Provider Condition 3.6 corresponds to GC C9.10.

- Existing telephone numbers and websites.
- Directors and persons of significant control (taking into account Companies House guidance).[34]
- Contact details for a senior individual with responsibility for authorising the messages.

2.90 We also expect providers to verify that any information they receive about the business sender corresponds with information available publicly about the business sender. As part of the information providers collect on the nature of business senders' activities, they must enquire about the purposes for which business senders expect to send A2P messages. They can use this information to help corroborate the legitimacy of alphanumeric Sender IDs (see paragraphs 2.98-2.103) and target future KYT checks (see paragraphs 2.106-2.115).

2.91 The risk assessment should highlight whether any of the information that providers have assessed contains an indication that the business sender poses a risk of sending scam messages. One or more of the following may be considered indicators of a risk of scams:

- Inaccurate, vague or otherwise unclear information about the intended use of A2P messaging: for example, the intended use may not match the nature of the business or organisation.
- Incorrect or incomplete information (such as address information).
- Adverse information from a public database, such as the Cifas National Fraud and Insider Threat databases or the Financial Conduct Authority's (FCA's) list of unauthorised firms and individuals.
- Not using a UK IP address where the business purports to be based in the UK, or otherwise not using an IP address that corresponds to the geographic location in which the business purports to be based.
- Indication that the business sender is located in a country or geographic location identified (by a provider or third party) to be at high risk of scam activity.
- Signing up outside of business hours (scammers may try to access providers' services outside of business hours to circumvent checks).
- Name, address, postcode, IP address or other information matching a disabled or dormant account with the provider.
- The same email address being used to open multiple accounts.
- Use of a generic, non-business email address.
- Use of a virtual private network.

2.92 If the risk assessment identifies one or more indicators of a risk of scams, the provider must:

- Cancel the onboarding of the sender; or
- Carry out enhanced checks on the sender to further inform the risk assessment and satisfy itself that the risk of scam activity is low.

2.93 Examples of enhanced checks include:

[34] Companies House, 2025. Guidance: People with significant control (PSCs): How to identify and record the people who own or control your company.

- Checking the Companies House register to confirm:
    - Whether important information about the business has recently changed.
    - Whether a person acting as a director of the business has been disqualified.
    - The key details of all individuals with influence over the business, including owners and directors.
    - The details of all individuals who receive any share of the revenue the business sender generates.
    - The names and details of any parent or ultimate holding company of the business sender.
- Asking for undertakings from the business sender that no other party is operating in the capacity of a shadow director, as defined under the Companies Act 2006.
- Checking against the Cifas National Fraud and Insider Threat databases that the business, or associated individuals, are not registered.
- Checking against the FCA's Financial Services Register that the business sender and individuals with which the provider is communicating have permission to carry out regulated financial activities, if relevant.[35]
- Checking relevant Ofcom enforcement decisions and published sanctions, including those relating to Premium Rate Services (and sanctions imposed by the former Phone-paid Services Authority and its predecessors), breaches of numbering-related requirements, misuse of numbers and other relevant non-compliance with regulation.[36]
- Checking relevant UK regulators' websites[37] for information relating to any other previous enforcement cases against the company or individuals where the case related to scams or other misuse of telephone numbers.
- Checking if the business sender has links to any other active accounts or previously blocked accounts with the provider.
- Verifying details of the sender's place of business, including ensuring the geographic location matches the information the sender has provided.
- Checking the Individual Insolvency Register to see if individuals with influence, including owners and directors, have gone bankrupt or signed an agreement to deal with their debts.
- Checking relevant industry registrations, e.g. an FCA firm reference number.

2.94 We encourage mobile operators and aggregators to share information with other providers through intelligence-sharing mechanisms where they become aware of business senders that have been responsible for previous scam activity. Providers should not onboard potential customers if the provider has credible evidence that the potential customer has previously been involved in scam activity, or similar.

[35] FCA, The Financial Services Register
[36] Ofcom, Complying with article 16 of the PRS Order. Ofcom is now responsible for enforcement with regard to Premium Rate Services.
[37] For example, the ICO.

2.95 Providers must retain records of risk assessments and evidence of checks for a period of at least 3 years after the end of the contractual relationship (as set out in Table 3, below). They should also ensure their records are up to date.

Checks on the use of new alphanumeric Sender IDs

C9.11[38] Checks when allowing the use of any new Alphanumeric Sender IDs must include:

(a) due diligence checks to verify that the proposed use of Alphanumeric Sender IDs aligns with the information disclosed during Know Your Customer Checks on the Business Profile, including the stated purposes for seeking to access A2P Message services; and

(b) where applicable, reviewing the proposed use of the Alphanumeric Sender ID against policies in place under Condition C9.13.

The purpose of this requirement

2.96 Providers may offer business senders the option of sending messages that bear an alphanumeric Sender ID rather than a telephone number or short code.[39] This option is attractive to legitimate business senders, but scammers can use alphanumeric Sender IDs to impersonate trusted organisations and deceive mobile customers.

2.97 This requirement is intended to prevent scammers from using alphanumeric Sender IDs to mislead potential victims. It is both an up-front requirement and an ongoing one, which we expect providers to apply each time a new alphanumeric Sender ID is allocated. As well as preventing scammers from using alphanumeric Sender IDs, this requirement should also help providers to identify scammers.

Alphanumeric Sender ID checks

2.98 Where a business sender requests to use a new alphanumeric Sender ID (either at onboarding or a later stage), providers must review the request (and information they have collected on the business sender) to ensure it does not indicate that the sender poses a risk of sending scam messages or breaching any relevant policies of terminating mobile operators in relation to alphanumeric Sender IDs.

2.99 Providers must verify that the alphanumeric Sender ID a business sender is requesting to use aligns with the information the sender provided during KYC checks. In particular, we would expect providers to use this information to verify to a high degree of confidence that the sender is authorised to represent themselves using business or brand names they request to use in alphanumeric Sender IDs. Providers should not allow a business sender to use a brand name that they are not authorised to use to represent themselves.

2.100 Providers must also not allow a business sender to use an alphanumeric Sender ID for any new use that is not consistent with the purpose for which they are seeking to send A2P messages, as recorded in KYC checks.

2.101 In line with GC C9.14, providers must ensure that senders from which they receive A2P messages are required to promptly notify them of any changes in their business profile or

[38] Non-Provider Condition 3.7 corresponds to GC C9.11.

[39] Some organisations use short codes to send A2P messages. These are usually five to six digits (e.g. 12345).

change in the use of alphanumeric Sender IDs. We therefore expect that, where a sender's business model has evolved and they may wish to use previously approved alphanumeric Sender IDs for a different purpose, they should notify the provider of this change. Providers should, as required under GC C9.8 and GC C9.12(b), review this information and update the associated risk assessment accordingly.

2.102 Separately, terminating providers are required to communicate a policy on alphanumeric Sender IDs throughout their A2P supply chain (see guidance in paragraphs 2.129-2.138 below). Aggregators must review requests to use alphanumeric Sender IDs against these policies to ensure they comply. Providers may wish to automate some of these checks where it can support quicker identification, if these checks work as intended in accordance with GC C9.19.

2.103 Below, we set out two examples of scenarios where providers would need to perform alphanumeric Sender ID checks and their outcomes:

- A business sender called the 'Office of Communications' would like to send messages with the alphanumeric Sender ID 'Ofcom'. Upon review of the details provided about the organisation, it is clear that 'Ofcom' is the public-facing name of the organisation, that the name does not contravene any policies put in place by the terminating provider on protected IDs and has not been listed as a protected Sender ID registered by another organisation. The use is approved.
- A business sender called 'Village Hairdresser' would like to send messages with the alphanumeric Sender ID 'ParcelDelivery'. The recorded purpose for which the sender is accessing A2P messaging is to send one-time passcodes for users to enter as part of two factor authentication of their online account. The stated purpose does not match the request alphanumeric Sender ID, to an extent that it may be indicative of scam activity. The use is denied and the account investigated.

Know Your Traffic (KYT) checks

C9.12[40] Know Your Traffic Checks must include:

(a) monitoring and reviewing data on volume patterns; identifying new or different use of Alphanumeric Sender IDs or Telephone Numbers; and checking any information on or notifications of changes in Business Profiles, for any indicators of Scam activity, taking into account policies in place under Condition C9.13 and information obtained under Condition C9.9(a)(vii) and C9.14 (whichever is applicable);

(b) using any insights from Condition C9.12(a) to review and update any previous risk assessments, as appropriate; and

(c) where any indicators of Scams are identified under Condition C9.12(a):

(i) seeking appropriate evidence as to whether or not the A2P Messages are legitimate; and

[40] Non-Provider Condition 3.8 corresponds to GC C9.12.

(ii) blocking those A2P Messages where the Regulated Provider reasonably believes, based on their review of any evidence provided, that the relevant A2P Messages were intended to Scam the intended recipients.

The purpose of this requirement

2.104 These requirements are intended to ensure that providers are conducting effective KYT checks on an ongoing basis, to root scammers out of A2P channels. This should help address cases where, for example, scammers take control of a business sender's account or evade KYC checks.

2.105 GC C9.12 sets out the minimum features of KYT checks that mobile operators and aggregators must ensure are conducted. Providers may take further measures they consider appropriate.

KYT checks

2.106 Providers are expected to monitor a range of scam indicators. While each scam indicator may not individually identify a potentially high-risk business sender, a combination of indicators is more likely to do so. We expect that providers can automate most checks, subject to compliance with relevant data protection legislation (see paragraph 2.248-2.260). While the KYT checks in GC C9.12 do not require providers to access the content of relevant messages, providers may consider this appropriate on a case-by-case basis if, in doing so, they are satisfied they are complying with any other relevant legislation (see paragraph 2.249).

2.107 Monitoring and reviewing data on volume patterns that could indicate scam activity may include checking for:

- A significant and unprecedented increase in messages sent from a single business sender.
- A level of use that appears inconsistent with a business profile provided during KYC checks.
- A new or constant stream of messages being sent, which may be inconsistent with traffic patterns associated with other legitimate uses, such as for marketing campaigns or appointment reminders.

2.108 When monitoring for new or unusual use of alphanumeric Sender IDs or telephone numbers, providers could take into account whether:

- A business sender has sought to use an alphanumeric Sender ID that does not align with its stated business purpose or appears to contravene a terminating provider's policy on protected Sender IDs.
- There has been a significant and unprecedented increase in applications from a business sender for alphanumeric Sender IDs or new telephone numbers.
- Available intelligence indicates that particular alphanumeric Sender IDs are being used in a malicious or deceptive manner, but have not yet been incorporated into the provider's Sender ID policies or controls.

2.109 Providers could monitor for changes in business profile information that business senders provide that may indicate potential scam activity, by checking for:

- Significant or multiple changes to information that the business sender provided under initial KYC checks.
- New details linked to the company appearing on registers (such as the Cifas National Fraud and Insider Threat databases or the Financial Conduct Authority (FCA) Warning List of unauthorised firms.[41]
- Changes where companies have been re-domiciled (in particular, where the relevant country, or geographic location, is known to be used by organised criminals to send scam messages).

2.110 Other activity that providers could perform to enhance their KYT checks includes:

- Monitoring the most-used Sender IDs across their traffic.
- Spot checks on end-users and on downstream aggregators, to ensure due diligence is being conducted.
- Conducting regular reviews with account holders.

2.111 Providers must review and update past risk assessments they hold on the business senders with which they contract if they encounter information relevant to that assessment in the course of undertaking KYT checks.

2.112 Providers should take into account any false positives identified through the systems and processes implemented under GC C9.26 (or otherwise). Where relevant, they should feed this information back into scam prevention and KYT processes to improve the effectiveness and accuracy of future monitoring and risk assessments.

2.113 Where a provider encounters scam indicators from a business sender in the course of conducting KYT checks, the provider should investigate whether messages from that sender are legitimate or contain scams. Where messages have been passed from another company that is not the business sender, we expect providers to engage with relevant companies in their supply chain to seek further information. Where the provider holds the direct relationship with the business sender, we expect them to take appropriate steps to obtain relevant information from the sender to enable the provider to satisfy itself that the messages are legitimate.

2.114 Where a provider reasonably believes, based on their review of the evidence, that the business sender has sent A2P messages that were intended to scam people, they must block that sender from sending further messages.

2.115 We also encourage mobile operators and aggregators to establish intelligence-sharing mechanisms (for example, through contractual requirements and/or amnesties for aggregators to report fraudulent traffic) for the purpose of reducing the likelihood that consumers receive scam mobile messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law. We also encourage providers to share information with other companies in their supply chain on tactics for detecting and assessing potential scam activities (see paragraphs 2.74-2.76).

[41] FCA Warning List of unauthorised firms.

Contractual requirements

C9.9[42] Regulated Providers must:

(a) implement and maintain clear and unambiguous contractual terms with any party from which they receive A2P Messages (that is not a Business Sender), requiring that party to:

(i) conduct Know Your Customer Checks on Business Senders at the Onboarding Stage, or take appropriate steps to ensure these checks have been conducted at the Onboarding Stage;

(ii) conduct checks when allowing a Business Sender to use a new Alphanumeric Sender ID to ensure that any proposed use of the Alphanumeric Sender ID is consistent with the Business Profile and purposes disclosed during Know Your Customer Checks, or take appropriate steps to ensure these checks have been conducted;

(iii) conduct on-going Know Your Traffic Checks on Business Senders or take appropriate steps to ensure these checks are conducted;

(iv) not transfer A2P Messages or enable the use of the relevant Alphanumeric Sender IDs unless they are reasonably satisfied with the checks carried out under Conditions C9.9(a)(i)-(iii);

(v) take appropriate, effective and prompt action in response to any reports of A2P Messages coming from their service that are suspected of being sent with the intention to Scam the recipients;

(vi) retain records in line with Conditions C9.21 to C9.25; and

(vii) take appropriate steps to ensure that Business Senders notify the party of changes to a Business Sender's Business Profile, or otherwise ensure that the party with the direct relationship to the Business Sender will be notified of such changes.

(b) implement and maintain appropriate and effective policies, systems and processes to:

(i) ensure ongoing compliance with the contractual obligations imposed under Condition C9.9(a);

(ii) monitor and assess compliance with these obligations, taking into account Conditions C9.16 and C9.19; and

(iii) take appropriate, effective and prompt action to address any non-compliance and, if applicable, satisfy itself the party will comply in future.

The purpose of the contractual requirements

2.116 This requirement applies where mobile operators or aggregators receive messages from other parties that are not the business sender (for example, where one aggregator receives messages from another, or where an aggregator receives messages from an MSP).

2.117 These requirements are intended to ensure that the required checks are carried out at the onboarding stage, irrespective of which party is onboarding the business sender, and that

[42] Non-Provider Condition 3.5 corresponds to GC C9.9.

appropriate incentives exist to ensure compliance. In essence, it should ensure that the obligation to carry out the required checks is passed down the contractual chain to the party that has a direct relationship with the business sender.

Setting clear and unambiguous terms

2.118 Where the provider is not directly involved in onboarding a business sender, they must set clear and unambiguous terms for the party from which they receive the A2P messages to either: undertake the KYC, alphanumeric Sender ID and KYT checks identified in GC C9.8; or ensure that these checks have been conducted by a party in the downstream chain. These terms must include provisions covering the requirements in GC C9.9(a), including provisions to ensure that parties take action in response to reports of scam messages coming from their services and to ensure they retain records.

2.119 Providers must also require the party from which they receive the A2P messages to either: take appropriate steps to ensure that business senders notify that person when there are changes to their business profile; or otherwise ensure that the business sender will notify the party in the message chain with which they have a direct relationship of such changes.

2.120 We expect the outcome of these requirements to be that, in all instances, when information that a business sender has provided in KYC checks changes, the party that conducted the KYC checks will be notified and can use insights to review and update any previous risk assessments, including in accordance with GC C9.12(b).

2.121 Downstream parties can help ensure that further downstream checks have been carried out by including similar requirements in their contracts.

Ensuring compliance

2.122 Providers are required to ensure that these contractual terms are complied with, on an ongoing basis. We expect them to ensure this by, for example, monitoring the activities of parties they contract with and undertaking appropriate incident management (see paragraphs 2.148-2.162). Providers may also need to communicate to ensure that the party with the direct contractual relationship with the business sender and present at the onboarding stage is subject to the relevant terms and conducts relevant checks.

2.123 Providers must take action to address non-compliance when it is identified. It is for providers to decide what strategies to employ to achieve compliance and to be able to demonstrate that they are effective. This could include imposing financial penalties under their contracts or placing restrictions on downstream parties' ability to convey certain types of messages.

2.124 If, after action has been taken to address non-compliance, that non-compliance continues and the provider is not satisfied that it is being addressed, we would expect that provider to cease to accept messages from the offending party. It is also open to providers to report potential non-compliance to Ofcom.

2.125 As explained in Section 3 below, Ofcom will have the power to take enforcement action for potential non-compliance and will decide whether, and against which provider(s), to take enforcement action in the circumstances. In making this decision, we will take into account our Regulatory Enforcement Guidelines.

2.126 We are more likely to take action against the provider we consider primarily responsible for any non-compliance but may also take action against other providers we consider have failed to take appropriate steps, such as those set out in paragraphs 2.67- 2.124, to prevent scam messages from being sent, in accordance with our GCs.

Setting a policy on protected alphanumeric Sender IDs

C9.13[43] Regulated Providers must implement and maintain appropriate and effective policies, systems and processes that impose restrictions on the use of Protected Alphanumeric Sender IDs in A2P Messages they terminate and communicate such policies to parties from whom they received A2P Messages, with the objective of preventing their use for Scams.

Who this obligation applies to

2.127 GC C9.13 applies to any Communications Provider that terminates A2P Messages.[44] GC C9.13 applies to mobile operators that enable A2P termination to their customers (including MNOs and some thick MVNOs). This obligation does not apply to MVNOs that do not have their own SMSC and/or rely on their host MNO to terminate A2P Messages.

The purpose of this requirement

2.128 Some types of alphanumeric Sender IDs may pose greater risk to end-users than others if scammers are successful in gaining access to them. These include recognised household brands or trusted organisations. Scammers may seek to copy these names directly in the Sender IDs they use or find other ways to imitate them (for example, by replacing a letter with a number). This requirement is intended to prevent scammers from impersonating existing organisations.

Setting a policy on protected alphanumeric Sender IDs

2.129 Our rules require mobile operators that terminate A2P messages to implement and maintain appropriate and effective policies, systems and processes to impose restrictions on the use of certain types of alphanumeric Sender IDs.

2.130 Downstream providers are not required to set a policy but are expected to take into account terminating providers' policies when approving the use of Sender IDs, in accordance with GC C9.11.

2.131 We expect policies under GC C9.13 to cover use of:

- **Protected brand IDs**: IDs that relate to high-risk known brands, which the terminating provider determines must not be used by any party other than the authorised brand.
- **Generic IDs**: IDs that the terminating provider prohibits because they are generic and could be used to mislead mobile customers about the sender.
- **Special alphanumeric characters**: an explanation of the alphanumeric character set that is either approved for use or prohibited.

2.132 Policies should be based on the terminating provider's assessment of the risk of harm posed by each alphanumeric Sender ID.

2.133 When considering how to list and protect brand IDs, we encourage terminating providers to:

- Consider high profile brands and organisations in sectors commonly targeted by scammers (for example banks, delivery companies and public bodies).

[43] Non-Provider Condition 3.9 corresponds to GC C9.13.
[44] See Condition 3.1(c) for the scope of the corresponding Non-Provider Condition (Condition 3.9)

- Take account of existing initiatives designed to prevent impersonation. Such initiatives may include the SMS Sender ID Protection Registry operated by the Mobile Ecosystem Forum.
- Proactively share their policy and lists with other terminating providers.

2.134 When considering which generic IDs to prohibit, we encourage terminating providers to focus on IDs that do not represent a specific brand, sub-brand or recognised name of the sender, and in particular to consider generic IDs that could form part of scammers' tactics. This includes words that:

- May appear familiar to recipients, such as 'Customer service' or 'Accounts'.
- Might convey urgency to the recipient, such as 'Alert', 'ActionNeeded' or 'Security'.
- Relate to banking or financial transactions, such as 'Payment', 'Bank' or 'Transfer'.
- Relate to online account security, such a 'SignIn', 'OTP', '2FA' or 'Code'.

2.135 When considering which alphanumeric characters to allow or prohibit, we encourage terminating providers to operate with a bias towards restricting the character set to those that are essential for legitimate business purposes. This could include, for example, prohibiting characters other than the standard alphabet, 0-9 numerals and essential punctuation. In particular, terminating providers should consider characters that could be used as substitutes for those in the standard alphabet, including those bearing accent punctuation or from non-Latin alphabets like the Greek alphabet.

2.136 As set out under GC C9.19, providers must keep their policies under review.

2.137 To comply with the requirement, we expect terminating providers to take reasonable steps to ensure that their policies are communicated to aggregators and MSPs. Providers could consider incorporating their policy into their contractual agreements.

2.138 To ensure these policies are enforced effectively and that all terminated messages are compliant, providers should consider implementing appropriate checks on their network. We also expect providers to have a feedback mechanism to alert downstream providers to messages they have passed on that have been found to include non-compliant alphanumeric Sender IDs.

Requiring notification of changes to business profiles

C9.14[45] Regulated Providers must take appropriate steps to ensure that Business Senders from which they directly receive A2P Messages are required to promptly notify them of any changes in their Business Profile, or changes in the use of any Alphanumeric Sender IDs.

Who this obligation applies to

2.139 GC C9.14 applies to any Communications Provider that transfers and/or terminates A2P Messages (including all Aggregators) and that receive A2P Messages directly from the business sender.[46] GC C9.14 applies to mobile operators (MNOs and some thick MVNOs) and all aggregators that contract directly with business senders.

[45] Non-Provider Condition 3.10 corresponds to GC C9.14.
[46] See Condition 3.1(b) for the scope of the corresponding Non-Provider Conditions (Condition 3.10).

The purpose of this requirement

2.140 In order to assess whether changes to information about a business sender potentially indicate scam activity and determine whether risk assessments need to be updated, providers must ensure that they are notified of these changes.

Ensuring notification of changes

2.141 To achieve this, we expect providers to set contractual obligations for business senders from which they receive messages directly, which place obligations on the business sender to notify the provider of changes to their business profiles. This includes any information that was collected during KYC checks that has since changed, including the purpose for which a business sender is accessing A2P messaging services.

2.142 Changes should be taken into account during KYT checks and previous risk assessments must be updated as appropriate in accordance with GC C9.12.

2.143 Where a provider does not receive messages directly from a business sender, but from an intermediary, C9.9 requires them to ensure that the onboarding party has contractual terms to the same effect.

Incident management requirements

C9.15 Where a Regulated Provider becomes aware of a Business Sender that they Onboarded sending or attempting to send, directly or indirectly, an A2P Message that the Regulated Provider reasonably believes was intended to Scam the recipient, the Regulated Provider must take the following steps within 1 Working Day:

(a) confirm the identity of the Business Sender responsible for those messages; and

(b) implement appropriate measures to prevent the Business Sender from sending further A2P Messages via any network or service the Regulated Provider provides unless the Regulated Provider has obtained evidence which they are satisfied demonstrates either:

(i) the Business Sender was not responsible for sending the relevant A2P Message; or

(ii) the relevant A2P Message was not intended to Scam the recipients.

C9.16 Where a Regulated Provider becomes aware of a Significant Scams Incident involving a Business Sender that they did not Onboard, the Regulated Provider must:

(a) within 2 Working Days in cases involving no more than one Aggregator or 5 Working Days in all other cases:

(i) take appropriate steps to confirm the identity of the Business Sender responsible for those messages; and

(ii) implement appropriate measures to prevent the Business Sender from sending further messages via any network or service the Regulated Provider provides unless they have obtained evidence which they are satisfied demonstrates either:

1. the Business Sender was not responsible for sending the relevant A2P Messages; or
2. the relevant A2P Messages were not intended to Scam the recipients;

(b) promptly within 15 Working Days:

(i) establish whether the party involved in delivering the relevant A2P Messages to the Regulated Provider is complying with the requirements that Regulated Provider imposed on them under Condition C9.9(a); and

(ii) take appropriate and effective action to address the non-compliance and, if applicable, satisfy itself the party will comply in future.

Who this obligation applies to

2.144 GCs C9.15 and C9.16 apply to any Communications Provider that transfers and/or terminates A2P Messages, including all Aggregators.[47] These GCs apply to mobile operators (including MNOs and some thick MVNOs) and aggregators (whether they are acting at tier 1 or at lower tiers). This obligation does not apply to MVNOs that do not have their own SMSC and/or rely on their host MNO to transfer and terminate A2P Messages.

The purpose of incident management requirements

2.145 These requirements are intended to govern how mobile operators and aggregators must respond when they become aware of scam messages that have been transferred through A2P channels. They should ensure that providers identify the source of the scam messages and prevent scammers from sending further messages.

2.146 The requirements are further intended to ensure that appropriate steps are taken where downstream providers have not complied with regulatory requirements or contractual obligations, which might have prevented the incident. Together, these actions will make protections on A2P channels more robust.

2.147 These requirements differ from KYT requirements under GC C9.12. Under the incident management requirements, providers must take action where the provider *reasonably believes scam messages have been sent* (whereas under the KYT requirements, providers must take action where KYT checks reveal *any indicators* of scam activity). Providers may reasonably believe scam messages have been sent because, for example, specific messages have been reported to them by end-users or by another provider.

Confirming the business sender responsible for sending scam messages

2.148 Where a provider has a direct relationship with a business sender and identifies a link to scam activity, we expect that the provider will confirm the business sender account responsible for sending a scam message directly. This must take place within one working day. We expect providers will need to confirm the business sender account responsible for the relevant messages to rule out the possibility that they originated from a different source, or because a business sender may send messages (including scam messages) from more than one alphanumeric Sender ID.

2.149 Where a provider does not have a direct relationship with the business sender, we expect the provider will need to ask downstream providers to share information to confirm the business sender responsible for the messages. This must be done within two working days in cases involving no more than one aggregator or five working days in all other cases.

2.150 Providers without a direct relationship with a business sender must act to confirm the business sender responsible when they are aware of a Significant Scams Incident, which we

[47] See Condition 3.1(b) for the scope of the corresponding Non-Provider Conditions (Conditions 3.11-3.12).

define as a situation where it appears to the provider that a particular business sender has cumulatively sent, or attempted to send, directly or indirectly, at least fifty A2P messages that the provider reasonably believes were intended to scam the recipients.

Preventing the business sender from sending further messages

2.151 Where a provider has a direct relationship with a business sender linked to scam messages, they must implement appropriate measures to prevent the business sender from sending further A2P messages via any network or service the provider provides. However, this requirement does not apply if the provider has obtained evidence that they are satisfied demonstrates that the business sender was not responsible for sending the relevant A2P message or the relevant A2P message was not intended to scam the recipients.

2.152 We would expect appropriate measures to include pausing access to services and providing an opportunity for the business sender to explain any legitimate mitigating circumstances. If legitimate mitigating circumstances apply (for example, if scammers have gained access to the business sender's account), the provider would be expected to seek proof and reassurances that reasonable measures are being taken to prevent future occurrences. Providers would also be expected to consider stronger checks in future (e.g. more frequent or intensive KYT checks on that business sender's account).

2.153 Where a provider seeks information from a business sender in order to assess whether messages were intended to scam recipients and the business sender does not respond, the provider should take reasonable steps to obtain that information. If, following these steps, the business sender has not responded, we would generally expect the provider to take that into account as a relevant factor when assessing the risk of scam activity they may pose. In such circumstances, it may be difficult for the provider to satisfy itself that the risk of future scam activity is sufficiently low to justify restoring the business sender's services.

2.154 However, we do not require providers to continue to withhold services from the business sender in every case where a business sender is unable to demonstrate that messages were legitimate, or where the provider is unable to obtain a response from the business sender. Providers should obtain appropriate evidence, take all relevant circumstances into account and exercise their judgement when determining whether restrictions should remain in place. It may be reasonable to give weight to indicators suggesting the messages are legitimate, even where there is no definitive evidence demonstrating this. We expect providers to take a consistent approach when assessing such cases.

2.155 If no legitimate mitigating circumstances apply, we expect providers to check whether the business sender has other accounts and put similar restrictions on these. They could also consider sharing intelligence with other trusted partners, taking into account the intelligence-sharing guidance in paragraph 2.28.

2.156 Where a provider does not have a direct relationship with a business sender, they must implement appropriate measures to prevent the business sender(s) from sending further messages via any network or service the provider supplies, unless they have obtained evidence that they are satisfied demonstrates that the business sender was not responsible for sending the relevant A2P messages (for example, because their account had been compromised temporarily) or that the relevant A2P messages were not intended to scam the recipients.

2.157 We would expect a check to include confirmation from downstream providers that service has been paused, or evidence of mitigating circumstances where it has not. Service could be

paused within two working days where there is up to one aggregator between that provider and the business sender (this could include up to one aggregator and one MSP), or five working days where there is more than one aggregator between the provider and the business sender. Where service has been paused but evidence of legitimate mitigating circumstances is later forthcoming, we expect providers to take this into account and promptly consider reversing measures taken.

Establishing whether other parties have conducted appropriate checks and are taking appropriate action

2.158 Where a provider does not have a direct relationship with a business sender, the provider must also (within 15 working days): establish whether the party involved in delivering the relevant A2P messages to the provider is complying with the relevant contractual requirements imposed on it under GC C9.9(a); take appropriate and effective action to address the non-compliance; and, if applicable, satisfy itself the party will comply in future.

2.159 To comply with this requirement, we would expect the provider to:

- Check whether the party that carried out the onboarding conducted initial and ongoing checks on the business sender and its traffic. This should include confirmation that KYC checks, checks relating to the use of alphanumeric Sender IDs and KYT checks were conducted, which could include relevant records of activity on that account.
- Seek credible reassurances, where the downstream provider does not provide evidence that it conducted appropriate checks, that this will be addressed. If the provider receives no credible reassurances, it should consider ceasing to accept traffic from the downstream provider until it provides these.
- Take into account any relevant past incidents and, where a downstream party appears to pose a higher risk, reflect this in their decision making.

Sharing information for incident management purposes

2.160 We recognise the possibility of information on legitimate customers being shared as part of how providers comply with incident management requirements (GC C9.16). For example, following a suspected incident, our measures require upstream aggregators to obtain evidence from downstream partners about the relevant business sender and to satisfy themselves that the incident was not the sender's fault or that it was not a scam.

2.161 In complying with these requirements, providers may wish to redact documents or set retention rules to protect customer data where possible, while also permitting effective incident management processes.

2.162 When assessing what information may be considered necessary to share to comply with our incident management requirements, we expect providers to take into account the following principles:

- Downstream providers should only need to share the minimum information necessary to inform upstream providers of the legitimacy of a business sender (or relevant A2P message).
- Upstream providers should only use information provided to them for the specific purpose for which it has been provided and should not pass it on to any other parties (in particular sales or marketing functions, including within subsidiaries or partners) for whom such information could provide a competitive advantage.

- Where considered appropriate, providers should restrict access to information both internally and externally: for example, by implementing confidentiality safeguards and/or contractual arrangements relating to data sharing to ringfence the information that is provided by downstream parties, including MSPs.
- Keeping a brief record of what is shared, with whom, why, and the expected outcome (as well as any confidentiality or data sharing agreements providers implement).

Guidance on the general cross-cutting measures

2.163 This section sets out guidance on a number of additional obligations that apply across all P2P and A2P messaging measures and therefore to all mobile operators and aggregators (as applicable). The guidance covers how providers may meet their obligations to:

- Implement and maintain appropriate and effective policies, systems and processes that enable an affected person to challenge any blocking of a message or number taken under GC C9.3 or C9.7 (GC C9.17)
- Have an accessible and reasonably prominent policy explaining the right to challenge, including on their website (GC C9.18).
- Regularly review their policies, systems and processes implemented under GC C9 to confirm that they remain appropriate and effective and are operating as intended (GC C9.19).
- Ensure that all relevant staff are trained on the policies, systems and processes in place under Condition C9, including on the right to challenge (GC C9.20).
- Implement and maintain appropriate record keeping policies, systems and processes (GCs C9.21 -25).
- Implement and maintain appropriate and effective policies, systems and processes to identify and monitor false positives under GCs C9.3(b) and (c) and C9.7 and take appropriate, effective and prompt action when these are identified (GC C9.26).
- Ensure they comply with relevant data protection legislation (GC C9.27).

Right to challenge requirements

C9.17[48] Regulated Providers must implement and maintain appropriate and effective policies, systems and processes that enable any affected person to challenge any blocking of a Mobile Number or message under Conditions C9.3 or C9.7.[49] The policies must:

(a) explain the circumstances under which any blocking may occur;

(b) explain how the person may challenge the blocking;

(c) explain the process the Regulated Provider will follow to investigate and determine any challenges made under Condition C9.17, including the evidence it is likely

[48] Non-Provider Conditions 3.13-3.14 correspond to GCs C9.17-C9.17

[49] For the avoidance of doubt, Regulated Providers are not required to treat challenges under Condition C9.17 as also 'Complaints' for the purpose of Condition C4 (that relates to complaints handling and dispute resolution processes).

to require from the person to demonstrate the Mobile Number or messages should not have been blocked;

(d) identify the different potential outcomes that may follow any challenge;

(e) identify conditions the Regulated Provider may attach to an outcome following a challenge, including any ongoing requirements that may be placed on the person;

(f) identify a prompt and reasonable timeframe within which the Regulated Provider will reach an outcome following a challenge; and

(g) explain the process the person may follow to appeal any decision not to remove any blocking taken.

C9.18 Regulated Providers must ensure that the policies, systems and processes in place under Condition C9.17 are well publicised and readily available, including ensuring that they are:

(a) easily accessible and reasonably prominent on their website; and

(b) referred to in the terms and conditions for all relevant products and services.

Who this obligation applies to

2.164 GCs C9.17 to C9.18 apply to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (except Lower-Tier Aggregators) and/or, in the context of P2P Messages, any Communications Provider that has assigned Mobile Numbers.[50] These GCs apply to all mobile operators (MNOs and all MVNOs) and tier 1 aggregators that block numbers or messages under GCs C9.3 or C9.7.

The purpose of the right to challenge requirements

2.165 The right to challenge requirements should ensure that there is a clear and accessible way for people affected by blocking of messages or numbers to challenge the decision, particularly in cases where messages and numbers may have been blocked in error.

2.166 While we consider that the risk that our measures will result in blocking of legitimate messages (i.e. false positives) is low and that taking the other measures set out in this guidance should mitigate the risk that false positives arise, we recognise that some false positives will still arise. Where they do arise, we consider the right to challenge to be an important protection.

2.167 We consider the right to challenge to be particularly important where false positives arise from automated monitoring of the content of messages under GCs C9.3 and C9.7.

Enabling people to challenge any blocking of messages or mobile numbers

2.168 Providers are required to implement and maintain appropriate and effective policies, systems and processes that enable any person to challenge any blocking of numbers or messages under GC C9.3 or C9.7 that affects them.

2.169 We expect providers to be transparent with all users about the processing of personal data they carry out in order to comply with GC C9.3 and C9.7 (including the possibility that messages may be blocked). We expect this information to be displayed clearly and prominently in an appropriate place on their website and in any terms and conditions or

[50] See Condition 3.1(d) for the scope of the corresponding Non-Provider Conditions (Conditions 3.13-3.14).

other information provided to customers. We understand providers should also be doing this to comply with data protection principles of fairness and transparency and this will provide senders with advance notice that their messages may be blocked. We also expect providers to help to inform end-users about how they can turn on delivery reports on their device (where available).

2.170 To ensure the right to challenge is an effective remedy, any person (senders, intended recipients and potentially other parties) can challenge a blocking decision under C9.3 or C9.7 that affects them.

2.171 A person whose message has been blocked, or who was expecting to receive a message, may not know which provider blocked it. Providers' policies should therefore enable any person to raise a challenge with their own provider or, where known, with the provider that applied the block.[51]

2.172 Where a provider receives a challenge from its own customer or an end-user whose number or message it has blocked, we expect providers to make reasonable efforts to review and resolve these cases without needing to engage with another provider. Any challenge will involve determining whether a message was intended to scam the recipient, or a number sent such messages, and in most cases this is likely to be straightforward.

2.173 We expect any review in relation to blocked messages to include the manual verification of the relevant message's content (taking into account relevant reports, such as to 7726, and associated traffic patterns). We also expect providers to carry out basic checks on any relevant URLs to assess their origin and credibility. Providers can request information they may need to be able to investigate from the challenger (e.g. name of sender, originating provider) and assess that information in the context of its own scam reports and other intelligence.

2.174 We expect that providers that have applied a block and received a related challenge to always resolve the challenge, because the blocking decision (and rationale) should have been based on that provider's judgment and information available to them. That provider should be able to review whether a number or message was blocked correctly.

2.175 Providers have discretion to decide how they will assess and determine challenges, but we expect them to take reasonable steps to obtain appropriate evidence, take all relevant circumstances into account and take a consistent approach. This means that, where a provider has a reasonable belief that a number or message is associated with a scam and the challenger cannot sufficiently demonstrate it is legitimate (and there are no other factors that suggest that their activity could be legitimate), the provider has the discretion to retain the block (it may also consider whether to report the matter to the police, if appropriate). Alternatively, if there are various indicators that a number or message is legitimate but no definite proof of its legitimacy,[52] the provider has discretion to remove the block.

[51] For example, on P2P channels, a sender can obtain confirmation from their provider on whether that provider applied the block. If they did not, it should be clear to the provider that the block was applied by the intended recipient's provider. On A2P channels, a sender may become aware that messages are being blocked by a particular provider because delivery failures are limited to that provider's network.

[52] For example, the sender ID or number aligns with known patterns used by a legitimate organisation, the message does not display typical characteristics of scams (e.g. no urgency or suspicious links) and the sender or number does not appear in scam reports.

2.176 Where a provider considers it necessary to communicate with another provider to comply with GC C9.17, it is unlikely that providers would need to transfer highly sensitive personal data between them. Where this may be considered necessary, we expect providers to comply with relevant data protection legislation[53] and to have regard to the guidance above on sharing information for incident management purposes at paragraphs 2.160-2.162.

2.177 Where a customer's provider cannot resolve a challenge because they did not apply the block, we would expect them to advise their customer (for example, that they are unable to remove a block). It may also be appropriate to advise the customer about what further action they may take (including raising a challenge directly with the provider that applied the block).

2.178 If a provider receives a challenge from an end-user that is not their customer about a block that the provider did not apply, the provider should confirm this promptly wherever possible, to resolve the challenge.

2.179 Providers must reach an outcome on challenges within a prompt and reasonable timeframe, and where appropriate and possible, should promptly remove a block on a number / unblock a message.

2.180 Providers' policies on the right to challenge are expected to at least include the requirements set out in Table 2, below.

Table 2: Summary of right to challenge requirements under GC C9.17 and guidance on how providers can comply

Minimum requirements of policies to enable the right to challenge	Guidance on how providers could comply
a) Explain the circumstances under which any blocking may occur.	Set out the reason(s) for the different circumstances in which a person's message or number may have been blocked in response to reports of scam activities.
b) Explain how the person may challenge the action taken.	Provide advice on how an end-user can raise a challenge: e.g. via a web form or email address.
c) Explain the process the regulated provider will follow to investigate the challenge, including the evidence it is likely to require from the person to demonstrate their message(s) or mobile number(s) should not have been blocked.	Set out the steps that the provider will follow to conduct their investigation. We would expect the provider to specify the team that will conduct the investigation, how they will contact the person to relay the outcome and what information/evidence they may need to enable the investigation to proceed effectively.

[53] Providers should take account of the ICO's guidance on sharing personal information when investigating scams and fraud. See ICO, Sharing personal information when preventing, detecting and investigating scams and frauds [accessed on 8 July 2026].

Minimum requirements of policies to enable the right to challenge	Guidance on how providers could comply
d) Identify the different potential outcomes that may follow any challenge to the actions taken.	We would expect one of the following scenarios to follow an investigation. The provider: • Maintains the block for example because: it continues to reasonably believe either that the relevant messages were intended to scam the recipients or the relevant number was responsible for sending scam messages, or the person does not share with the provider the information it requires to resolve the challenge within a specified timeframe. • Removes the block on a number/(where possible) unblocks a message and/or takes other action, because it no longer reasonably believes either that the relevant messages were intended to scam the recipients or that the number was responsible for sending scam messages. • Finds that it is unable to resolve the challenge because another provider has imposed the block. While providers are expected to make reasonable efforts to resolve a challenge on behalf of their customer, it may be appropriate to advise their customer about why they are unable to remove a block. It may also be appropriate to advise the customer about what further action they may take (including raising a challenge directly with the provider that applied the block). • Is notified that the person has withdrawn their challenge.
e) Identify conditions the Regulated Provider may attach to an outcome following a challenge, including any ongoing requirements that may be placed on the person.	Where a provider receives a challenge from a person whose number or messages it has blocked, the provider may consider it appropriate to only continue to accept messages from that person if certain conditions are met. These conditions may, for example, relate to that person's processes, its customers or the volume of messages it may be allowed to send in the future.

Minimum requirements of policies to enable the right to challenge	Guidance on how providers could comply
f) identify a prompt and reasonable timeframe within which the Regulated Provider will reach an outcome following a challenge.	We would expect the provider to identify a prompt and reasonable timeframe in which it aims to reach a decision following an investigation and to inform the person of that timeframe (e.g. within a certain number of working days). When considering timeframes for an investigation, we also expect providers to take into account specific circumstances, including the type and extent of the evidence that a number or message was legitimate or that the relevant messages are time-sensitive, such as appointment reminders.
g) Explain the process the person may follow to appeal any decision not to remove any blocking.	Point them in the direction of any processes that allow the person to escalate their challenge. This could include any existing complaints process used by the provider.

2.181 Providers must ensure they act in accordance with their right to challenge policy.

2.182 Relevant staff should be appropriately trained on the right to challenge (see paragraphs 2.200-2.201, below).

2.183 Providers must also ensure the policies, systems and processes they have in place under GC C9.17 are well publicised and readily available, including ensuring that they are:

- Easily accessible and reasonably prominent on their website. We expect provider's website (or corresponding apps) to clearly identify and explain the right to challenge policy. Providers should also consider having these in FAQs.
- Referred to in the terms and conditions for all relevant products and services.

2.184 We expect a right to challenge policy to be clear and comprehensible. Providers are also expected to make these policies available in hard copy (or alternative formats) free of charge on reasonable request. This includes providing the policy in a reasonably acceptable format, such as large print and Braille, in response to requests from customers who require this.

Review of policies, systems and processes

C9.19[54] Regulated Providers must regularly review their policies, systems and processes, implemented under Condition C9 to ensure that:

(a) they remain appropriate and effective and are operating as intended;

(b) the Regulated Provider is complying with its policies, systems and processes; and

(c) any issues identified are promptly and effectively addressed, including by making appropriate changes to their policies, systems and processes implemented under Condition C9.

[54] Non-Provider Condition C3.15 corresponds to GC C9.19.

Who this obligation applies to

2.185 GC C9.19 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (including all Aggregators), and/or has assigned Mobile Numbers.[55] GC C9.19 applies to all mobile operators (MNOs and all MVNOs) and aggregators (whether they are acting at tier 1 or at lower tiers).

Purpose of reviewing policies, systems and processes

2.186 The purpose of this requirement is to ensure that providers maintain the effectiveness of anti-scam measures. If providers do not remain vigilant to new and emerging threats, their systems and processes are likely to become less effective.

Conducting reviews of anti-scam policies, systems and processes

2.187 Providers must review their policies, systems and processes (including all rules) implemented under GC C9 regularly to confirm that they remain appropriate, effective and are operating as intended. They must also ensure they are complying with their own policies, systems and processes.

2.188 We expect reviews to include both:

- Informal reviews, as part of an ongoing evaluations of threats. We expect providers to carry these out on a continual or ad hoc basis, in response to any new threats, incidents or challenges that may arise.
- More formal and comprehensive reviews or audits, which we expect providers to carry out less frequently, for example annually, depending on the nature and extent of any informal reviews.

2.189 The timing and extent of each review will depend on the circumstances, including the policy, system or process that is under review and whether it is a more or less formal review. It will be appropriate to review some policies, systems and processes more regularly than others.

2.190 Providers may use more formal reviews to assess the overall effectiveness of their anti-scam measures. We would generally expect providers to carry out more formal reviews or audits at greater intervals than less formal reviews (for example, annually or potentially less frequently, depending on the nature and extent of any ongoing reviews).

2.191 It is for providers to decide what is reasonable and proportionate for their particular circumstances, including the frequency and type of review they carry out. We also expect providers to remain flexible and adapt the timing and extent of reviews where they become aware of new threats, incidents or challenges that may require more immediate assessment.

2.192 Examples of steps providers could take to support compliance with these requirements include:

- Reviewing scam intelligence frequently (e.g. daily) to support identification and blocking processes.
- Using a broad range of data sources to inform reviews and stay up to date on emerging threats and developments in cybercrime including through engagement with industry forums, law enforcement and anti-scam organisations.

[55] See Condition 3.1(b) for the scope of the corresponding Non-Provider Condition (Conditions 3.15).

- Periodically assessing sources of scam reports to maintain access to quality intelligence and identify new sources of value from appropriate third parties.
- Considering any learnings from challenges and false positives that are identified.
- Engaging solution vendors (e.g. firewall systems providers) and/or other competent third parties to support audits and inform reviews.
- Establishing cross-organisational working groups to coordinate learnings. This may include collaboration between specialist fraud teams and customer-facing functions in different organisations.
- Structuring working groups to support rapid responses to emerging threats and enable efficient implementation of updated measures.
- Facilitating coordination between MNOs and MVNOs to ensure insights into scam prevention are shared effectively.
- Communicating planned next steps clearly with relevant parts of the organisation following each review.
- Ensuring oversight by a senior individual of all reviews and audits.

Ensuring that issues are addressed promptly

2.193 Providers must take prompt and effective action to ensure that they address any issues they identify, including by making appropriate changes to their policies, systems and processes implemented under GC C9.

2.194 We would expect providers to meet this obligation by ensuring that relevant teams and individuals are equipped to respond to emerging threats quickly and that they document any findings from reviews clearly and share them with appropriate teams.

2.195 We would expect to see clear lines of accountability and responsibility agreed and communicated to relevant teams and individuals, so it is clear who needs to take action and when.

2.196 Guidance relating to the review of systems and processes for identifying, monitoring and addressing false positives is set out in paragraphs 2.229-2.245 below.

Training staff

C9.20[56] Regulated Providers must ensure that all relevant staff are appropriately trained on, the policies, systems and processes in place under Condition C9, including ensuring relevant staff are appropriately trained on the right to challenge processes implemented under Condition C9.17.

Who this obligation applies to

2.197 GC C9.20 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (including all Aggregators), and/or has assigned Mobile Numbers.[57] GC C9.20 applies to all mobile operators (MNOs and all MVNOs) and aggregators (whether they are acting at tier 1 or at lower tiers).

[56] Non-Provider Condition C3.16 corresponds to GC C9.20.
[57] See Condition 3.1(b) for the scope of the corresponding Non-Provider Condition (Conditions 3.16).

Purpose of training relevant staff

2.198 The purpose of this requirement is to ensure providers take the necessary steps to ensure their staff can effectively implement and comply with the applicable conditions in GC C9.

2.199 Relevant staff includes any staff that are or may be involved in implementing Condition C9. This includes technical and other staff working in specialist fraud prevention or network teams, as well as staff that handle challenges and enquiries relating to blocked numbers and messages (including customer-facing teams that are the first point of contact for a challenge or enquiry and staff to whom challenges may be escalated). It also includes any third parties or partners that carry out these functions on behalf of a provider.

Steps to ensure relevant staff are appropriately trained

2.200 Providers must ensure that all relevant staff are trained on the policies, systems and processes they have in place under Condition C9. We expect providers to ensure their policies, systems and processes are widely communicated within their organisation, including to customer-facing teams who are the first point of contact for a challenge or enquiry and staff to whom challenges may be escalated.

2.201 We expect the training provided to meet the objective of ensuring relevant staff have the appropriate skills, competencies and tools for the full design, implementation, operation and monitoring of the relevant requirements under GC C9. This includes ensuring that relevant staff receive appropriate training on:

- Validating scam reports and inputting rules into blocking tools.
- Identifying, monitoring and addressing false positives, including carrying out any human review of messages to determine whether its contents were intended to scam the intended recipient.
- Carrying out due diligence and ongoing KYT monitoring of A2P traffic.
- Responding to incidents arising on A2P traffic.
- The right to challenge processes implemented under GC C9.17:
    - Providers are expected to take appropriate steps to ensure that all customer-facing teams that deal with the right to challenge are trained to identify such challenges, know what internal teams to engage to help assess a challenge and what information and guidance to provide to challengers to enable them to navigate the process effectively.
    - Providers are also expected to ensure staff to whom challenges may be escalated have the appropriate skills to understand how the provider is expected to assess and determine challenges and, more generally, check whether the provider has acted in accordance with its right to challenge policy.

Record keeping requirements

C9.21[58] Regulated Providers must implement and maintain appropriate record keeping policies, systems and processes to demonstrate and ensure continued compliance with Condition C9. These must be overseen by a designated senior individual and must, where applicable, provide for the records identified in Conditions C9.22 to C9.25 below to be retained for at least the time period identified in those Conditions.

C9.22 The following records must be kept for a period of at least five years:

(a) records of policies, systems and processes implemented under Condition C9;

(b) records of reviews of the effectiveness of policies, systems and processes implemented under Condition C9, including any actions taken or changes made to those policies, systems and processes under Condition C9.19; and

(c) records of the description of an incident under Conditions C9.15 and C9.16 (including the date and time the incident was identified and the number of messages involved), and measures or actions taken in response to that incident.

C9.23 The following records must be kept for a period of at least three years after the end of the relevant contractual relationship:

(a) records of Know Your Customer Checks and checks relating to the use of Alphanumeric Sender IDs carried out under Condition C9.8, including initial and subsequent risk assessments;

(b) records of actions taken as a result of Know Your Traffic Checks carried out under Condition C9.8;

(c) records of requirements imposed on parties under Condition C9.9(a); and

(d) records of actions taken to ensure ongoing compliance and address any non-compliance under Condition C9.9(b).

C9.24 Records relating to False Positives under Condition C9.26 must be kept for a period of at least two years and must include:

(a) a description of a False Positive incident (including the date and time the incident first arose; its impact; the likely cause; and how and when it was identified); and

(b) any measures or actions taken in response to that incident.

C9.25 The following records must be kept for a period of at least one year:

(a) Records of communications between a Regulated Provider and any person regarding a challenge raised under Condition C9.17, from the date the challenge was resolved or otherwise closed; and

(a) records of each instance a Pay As You Go Customer reaches a volume limit set by the Regulated Provider under Condition C9.4 (including the Pay As You Go Customer's Mobile Number and the date on which that volume limit was reached).

[58] Non-Provider Conditions C3.17-C3.21 correspond to GCs C9.21-C9.25.

Who this obligation applies to

2.202 GCs C9.21 to C9.25 apply to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (including all Aggregators), and/or has assigned Mobile Numbers.[59] These GCs apply to all mobile operators (MNOs and all MVNOs) and aggregators (whether they are acting at tier 1 or at lower tiers), but some providers will only need to comply with a subset of the requirements, as relevant to their business. For example, aggregators will not need to comply with record keeping related to P2P measures provided they do not transfer or terminate such P2P Messages.

The purpose of record keeping requirements

2.203 The purpose of these record keeping requirements is to ensure that providers possess written documentation of the measures taken to comply with the requirements of GC C9. Clear and up to date records will also enable providers to monitor the ongoing effectiveness of their scam prevention measures and ensure they are complying with their obligations.

Record keeping requirements

2.204 Providers must implement and maintain appropriate record keeping policies, systems and processes to demonstrate and ensure continued compliance with GC C9. A designated senior individual with delegated authority or responsibility for compliance with GC C9 and/or fraud prevention must oversee providers' record keeping policies, systems and processes. This senior individual must, where applicable, provide for the records identified in GCs C9.22 to C9.25 to be retained for at least the time period identified in these Conditions.

2.205 The record keeping requirement includes keeping records of the categories of documents identified in Table 3, below. In accordance with Table 3, mobile operators within the scope of requirements relating to P2P messaging must keep records relating to:

- Policies, systems and processes implemented under Condition C9.
- Reviews of the effectiveness of those anti-scam measures.
- Instances where PAYG customers reach volume limits set.
- Communications relating to challenges to blocking measures.
- Identifying, monitoring and addressing false positives.

2.206 Mobile operators and aggregators within the scope of requirements relating to A2P messaging must keep records relating to:

- Policies, systems and processes implemented under Condition C9.
- Reviews of the effectiveness of those anti-scam measures.
- KYC checks and checks on alphanumeric sender IDs, including initial and updated risk assessments.
- Contractual terms and compliance with those contractual terms that they have agreed with parties from which they receive A2P messages.
- Measures taken as a result of KYT checks.
- Measures taken in response to incidents.

[59] See Condition 3.1(b) for the scope of the corresponding Non-Provider Conditions (Conditions 3.17-3.21).

- Communications relating to challenges to blocking measures.
- Identifying, monitoring and addressing false positives.

2.207 We set out further details on our expectations for some of these data retention requirements below.

Records of policies, systems and processes

2.208 For the purposes of GCs C9.22(a) and (b), we expect providers to retain records of their overarching policies, systems and processes, together with records of formal reviews of those policies, systems and processes and any resulting actions or changes.

2.209 The type of policies we expect to be retained under this requirement include providers' policies on their approach to:

- Receiving and validating scam reports.
- Identifying and blocking scam numbers and messages.
- Volume limits for PAYG customers.
- Due diligence and ongoing monitoring for A2P messages.
- Identifying, monitoring and addressing false positives.

2.210 Providers are also expected to keep records of how these policies comply with relevant data protection legislation.

2.211 Different requirements may be covered within a single policy document and providers should retain all versions of such policies for at least five years.

2.212 Providers are not required to retain records of individual messages that they have blocked, specifically. Further, we do not expect providers to retain day to day operational data under this requirement, such as frequently updated blocking rules, scam URL lists, scam number lists, firewall systems, configurations or other information that may change on a daily or hourly basis.

Records of volume limits for PAYG customers

2.213 For records relating to the application of volume limits under GC C9.25(b), providers are required to retain a record of each instance a PAYG customer reaches a volume limit set under GC C9.5, including:

- That customer's telephone number.
- The date on which that volume limit was reached.

2.214 If current systems delete underlying records before 12 months have elapsed, providers may need to periodically capture and retain the information necessary to comply with this requirement.

Records of incident management

2.215 For records retained under GC C9.22(c), providers are required to retain:

- A description of an incident under GC C9.16 and C9.16 (including the date and time the incident was identified and the number of messages involved).
- Records of the measures or action taken in response to an incident (which we expect to include the date such measures or actions were taken).

2.216 We expect this information could be retained in a standard template, form or incident log. We do not require providers to retain detailed operational or dynamic traffic data for the purposes of this requirement.

Records of KYT checks

2.217 GC C9.23(b) requires providers to retain records of actions taken as a result of KTY checks carried out under Condition C9.8. As explained in paragraph 2.113 above, such actions are likely to occur where a provider encounters scam indicators from a business sender. Where the provider cannot satisfy itself that the relevant messages were legitimate we expect providers to retain records of:

- The actions taken (for example, blocking a sender from sending further messages).
- The date the actions were taken.
- The name of the relevant business sender (and where relevant, the downstream provider that passed the messages to the provider).

Records of information on challenges

2.218 For records retained under GC C9.25(a), providers are required to retain records of communications between that provider and any person regarding a challenge raised under Condition C9.17, from the date the challenge was resolved or otherwise closed. This is the same type of information providers are already required to retain under paragraph 20 of the Annex to GC C4 relating to complaints. Taking into account the requirements of GC C4, we expect communications relating to challenges to include a clear record of the following information, or otherwise expect providers to ensure they have a clear record of the following information:

- The date on which a challenge was received.
- How the challenge was made (for example, by email or by phone).
- The identity and contact details of the person making the challenge.
- A description of what the challenge is about.
- All communications made or received between the provider and the person making the challenge regarding the challenge including, as a minimum:
  - The date on which the communication was made or received.
  - How the communication was made or received (for example, by email or by phone).
  - A description of what was contained in the communication (for example, advice given and/or action proposed to be taken and/or action agreed with the person making the challenge to be taken, to resolve the challenge).
  - Copies of any written communication.
- The date on which the challenge was resolved or otherwise closed.

2.219 For the purposes of this requirement, references to ‘challenges’ include any query regarding blocking activity made under the provider's processes implemented pursuant to GC C9.17 and are not limited to formal legal challenges.

Records of false positives

2.220 Providers that are subject to GCs C9.3(b) and (c) or C9.7 and therefore subject to GC C9.26 are required to retain:

- A description of a false positive incident including:
  - The date and time the incident first arose.
  - The impact of the incident (which we expect to include: how many messages were incorrectly blocked; the time period over which they were blocked; and the number of complaints or other known impacts).
  - The likely cause of the incident (which we expect to include information on whether the sole cause was likely to be implementing our requirements, or whether a provider reasonably believes a false positive may have arisen as a result of implementing our requirements).
  - How and when the incident was identified (which we expect to include the time and date on which it was identified).
- Any measures or actions taken in response to that incident, which we expect to include:
  - A record of any changes to rules, configurations or datasets.
  - The date and time on which such measures or actions were taken.

2.221 We also expect providers to retain information that enables them to assess trends over time, such as information on recurring issues or increases in the frequency or extent of false positives.

Retention periods for different categories of records

2.222 Providers must implement and maintain effective systems for keeping records for the minimum required period. These systems are essential for providers to demonstrate compliance with GC C9. These must be overseen by a designated senior individual.

2.223 The designated senior individual must make sure that all the specific records mentioned in C9.22 to C9.25 are kept for at least a specified length of time. The requirements in each case are summarised in Table 3.

Table 3: The minimum time periods required for providers to retain specific categories of records related to scam prevention policies

Retention period	Categories of records that providers must keep
12 months	• Communications relating to challenges under GC C9.17 (retention period starts after the challenge is concluded). • Instances where PAYG customers reach a volume limit set under GC C9.4.
2 years	• Description of false positive incidents and measures or actions taken in response to that incident under GC C9.26.

Retention period	Categories of records that providers must keep
3 years after the end of the contractual relationship	• KYC checks and checks on alphanumeric sender IDs (under GC C9.8), including initial and updated risk assessments. • Actions from KYT checks (under GC C9.12). • Requirements imposed on entities under GC C9.9(a) (to implement and maintain clear and unambiguous contractual terms with any party from which they receive A2P messages that is not a business sender). • Actions taken for ongoing compliance/addressing non-compliance with entities under GC C9.9(b).
5 years	• Policies, systems and processes implemented under GC C9. • Reviews of effectiveness of the policies, systems and processes, including any resultant actions or changes under GC C9.19. • Descriptions of incidents and measures or actions taken in response to incidents under GCs C9.15 and C9.16.

General expectations of record keeping

2.224 Providers may keep written records in a format and location of the provider's choice provided they are clear, comprehensible and easily accessible, so they can be easily and promptly supplied to Ofcom if requested.

2.225 Providers should also ensure their records (in particular records relating to long-standing customers) are kept up to date, taking into account the data accuracy principle in the UK GDPR.

Identifying, monitoring and addressing false positives

C9.26[60] Where a Regulated Provider is required under Conditions C9.3(b), C9.3(c) or C9.7 to block messages, the Regulated Provider must implement and maintain appropriate and effective policies, systems and processes to identify and monitor False Positives, and take appropriate, effective and prompt action when False Positives are identified.

Who this obligation applies to

2.226 GC C9.26 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, except Lower-Tier Aggregators.[61] GC C9.26 applies to MNOs, thick MVNOs and tier 1 aggregators that are required to comply with GCs C9.3(b) and (c) or C9.7, where false positives may arise as a result of blocking decisions under GCs C9.3(b) and (c) and C9.7.

The purpose of these requirements

2.227 The purpose of GC C9.26 is to ensure that providers have effective arrangements in place to identify, monitor and respond to false positives that may arise under GCs C9.3(b) and (c) and C9.7. While other requirements in this guidance are intended to reduce the likelihood of

[60] Non-Provider Condition C3.22 corresponds to GC C9.26.
[61] See Condition 3.1(d) for the scope of the corresponding Non-Provider Condition (Conditions 3.22).

false positives,[62] we recognise that providers cannot eliminate false positives entirely and they may arise for a range of reasons, including human error, inaccuracies in scam reports and/or inadequate validation of scam reports or limitations in blocking tools and processes.

2.228 Identifying and addressing false positives is important to mitigate the risk of interference with end-users' communications, particularly where end-users may not otherwise become aware that their messages have been blocked. GC C9.26 is therefore intended to ensure providers have appropriate systems and processes in place to detect false positives, take prompt corrective action and prevent recurrence.

Steps to identify and assess false positives

2.229 Providers can use automated tools and/or human review to help identify false positives through periodic reviews of blocked messages or traffic patterns. This may include reviewing sender IDs, numbers or campaigns against available information about known legitimate traffic to help identify potential false positives.

2.230 Providers may also use automated tools and/or human review to determine whether a block has resulted in a false positive. When assessing whether a false positive has occurred, we expect providers to consider a range of indicators, including the content of blocked messages, related scam reports, traffic patterns and any associated URLs or telephone numbers.

2.231 Providers should not rely on challenge mechanisms, queries or complaints as their primary means of identifying false positives, given that the number of challenges they receive may not reflect the true incidence of false positives.

2.232 Providers should recognise that they may be less likely to detect false positives in relation to certain types of traffic: for example, on P2P messaging, where some end-users may not be aware that a provider has blocked a message and may also be less likely than business senders to challenge blocking decisions. Providers should take this into account in their approaches to monitoring for false positives.

2.233 To help identify the occurrence of false positives on A2P traffic, providers should maintain working communications channels with other providers from which they receive or transmit messages, to enable rapid escalation where legitimate traffic may have been blocked in error and ensure such cases are investigated and resolved promptly.

Steps to monitor false positive trends

2.234 Providers should monitor trends in false positive rates over time, which will help them to identify unexpected increase that may indicate the emergence of a new source of false positives. Providers should also monitor such trends to identify recurring issues, emerging risks and potential weaknesses in identifying and blocking measures.

2.235 Providers may also wish to monitor trends across different traffic types, services, campaigns or blocking measures to help emerging issues more quickly.

---

[62] The risk of false positives should already be mitigated by a number of other requirements in GC C9. In particular, GCs C9.2 and C9.6 require providers to validate scam reports (where appropriate) before acting on them; GC C9.3 and C9.7 require providers to have “appropriate and effective” policies, systems and processes as well as reasonable grounds before blocking messages or numbers; GC C9.17 requires providers to provide a right to challenge blocking decisions; GC C9.19 requires providers to review their systems and ensure they are working as intended; and GC C9.20 requires providers to ensure relevant staff are appropriately trained. Together, these measures are intended to reduce the likelihood of false positives.

Steps to mitigate the impact of false positives and prevent reoccurrence

2.236 Where providers identify false positives, they must take appropriate, effective and prompt action. This is particularly important given the significant number of legitimate messages that they could potentially block in a short space of time if things go wrong (for example, due to human error). We expect providers to take action where they:

- Identify individual false positives.
- Observe an unexpected increase in false positive rates.

2.237 Appropriate action is likely to include ensuring the same legitimate messages or type of legitimate messages (e.g. message campaigns) are not blocked. This may require providers to amend rules in blocking tools and feeding false positives back into validation checks. We expect providers to carry out root cause analysis to understand why erroneous blocking has occurred and make appropriate changes to systems, processes and/or controls, including updating rules, filters or datasets to prevent a recurrence. Providers should also ensure that they document the findings of such reviews and share them with relevant teams.

2.238 We do not expect providers to unblock messages that they have blocked erroneously after finding them to be false positives (which could cause confusion to end-users). However, providers may do so where appropriate (and possible), for example following a challenge under GC C9.17.

Steps to keep systems under review

2.239 GC C9.19 requires providers to keep their policies, systems and processes under review. It also explains that providers may carry out informal reviews or more formal and comprehensive reviews or audits. The guidance below sets out how providers can ensure their arrangements for complying with GC C9.26, specifically, remain effective and appropriate.

2.240 Under one or more of the types of review providers may carry out, providers should assess the extent to which their policies, systems and processes are effective in identifying and minimising false positives.

2.241 This should include:

- Assessing available evidence on false positives, including any data, case reviews, or other indicators of false positives.
- Reviewing the outcomes of any proactive monitoring, challenges or sampling of blocked messages or campaigns.
- Identifying any recurring causes of false positives, such as issues with specific rules, thresholds, datasets or processes.

2.242 Where issues are identified, providers should ensure that:

a) Recurring or systemic causes of false positives are identified and understood.

b) Appropriate changes are made to systems, processes or controls, including updating rules, filters or datasets to prevent recurrence.

c) Where appropriate, the effectiveness of those changes is assessed subsequently to ensure the underlying issue has been addressed.

2.243 Providers should ensure that the findings of such reviews are documented and shared with relevant teams.

2.244 Providers may wish to adopt similar measures in relation to false positives that may arise as a result of blocking processes and decisions that go further than the requirements of GC C9.

Steps to ensure compliant record keeping

2.245 GC C9.21 requires providers to keep records of their policies, systems and processes for five years (see paragraphs 2.208-2.212). This includes providers' policies, systems and processes relating to identifying, monitoring and addressing false positives. GC C9.24 also requires providers to keep records of descriptions of false positive incidents and measures or actions taken in response to that incident for two years (see paragraphs 2.220-2.221).

Data protection requirements

C9.27[63] Condition C9 applies subject to the requirements of the Relevant Data Protection Legislation.

Who this obligation applies to

2.246 GC C9.27 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (including all Aggregators), and/or assigns mobile numbers.[64] GC C9.27 applies to all mobile operators (MNOs and all MVNOs) and aggregators (whether they are acting at tier 1 or at lower tiers).

The purpose of this requirement

2.247 The purpose of this requirement is to ensure providers comply with relevant data protection legislation when they are seeking to comply with GC C9.

Compliance with relevant data protection legislation

2.248 Many of our rules under GC C9 are likely to require providers to process personal data. This is because message senders, intended recipients or other individuals are identifiable from the content or metadata of a message, or the content or metadata of a message is connected to other information that renders someone identifiable. Such processing, in particular automated processing, can lead to a number of possible data protection harms, such as loss of control of personal data, invisible processing or unwarranted surveillance.[65] Also, a telephone number can arguably be information about an identifiable individual and therefore may also be considered personal data in certain circumstances.

2.249 Providers must therefore comply with the GCs in a way that ensures compliance with relevant data protection legislation. This includes:

- The UK GDPR.
- The Data Protection Act 2018 (DPA).
- The Privacy and Electronic Communications Regulations 2003 (PECR).

2.250 We also expect providers to take into account any relevant guidance issued by the ICO.

---

[63] Non-Provider Condition C3.23 corresponds to GC C9.27.
[64] See Condition 3.1(b) for the scope of the corresponding Non-Provider Condition (Conditions 3.23).
[65] See also ICO, 2022. Overview of Data Protection Harms and the ICO's Taxonomy.

2.251 The UK GDPR sets out seven key principles that sit at the heart of data protection law (and which providers will need to consider as part of ensuring their processing complies with data protection rules).[66] These are:

a) Lawfulness[67], fairness and transparency.[68]
b) Purpose limitation.[69]
c) Data minimisation.
d) Accuracy.[70]
e) Storage limitation.
f) Integrity and confidentiality (security).
g) Accountability.

2.252 The UK GDPR provides a higher level of protection for the processing of particularly sensitive categories of data relating to race, sexual orientation, sex life, health data, political opinions, trade union membership, religious or philosophical beliefs, biometric or genetic data (known as special category personal data) and criminal conviction and offence data.

2.253 Providers may also use third parties to carry out any data processing on their behalf. ICO guidance is clear that, where third parties are used, it is for the service provider and that third party to identify their respective roles and obligations under data protection law and ensure that all the requirements of that law are met.[71] Providers will also need to comply with the rules on "restricted transfers" in the UK GDPR if transferring personal data outside the UK for the purposes of implementing the GCs, ensuring that appropriate safeguards are in place with respect to all such transfers.

2.254 Other data protection legislation and guidance that are particularly relevant to complying with GC C9 includes rules and guidance relating to the monitoring of content, in particular automated monitoring. Providers should consider whether they are likely to be in scope of Article 22A UK GDPR relating to automated decision making, which applies where a provider makes decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. We note that the ICO's guidance on content moderation and data protection (in particular on "What if we use automated decision-making in our content moderation?")[72] indicates that content moderation will not involve solely automated decision making where it involves a database matching tool. Similarly, the

---

[66] Further information on these principles is available in ICO, A guide to the data protection principles [accessed on 8 July 2026]. See also ICO. What data protection rights do people have? [accessed on 8 July 2026].

[67] The UK GPDR and the Data Protection Act 2018 both contain specific provisions that support the sharing of personal data to prevent and detect crime, including fraud. For example, see Article 6(1)(ea) of the UK GDPR and paragraph 5(a) of Annex 1 to the UK GDPR.

[68] For example, providers should be transparent with users about the processing of personal data they carry out in order to comply with GC C9 (see paragraph 2.169).

[69] See ICO, Guidance on purpose limitation (March 2026) [accessed on 8 July 2026].

[70] For example, robust validation of scam reports and ensuring records are kept up to date will help ensure compliance with the data accuracy principle.

[71] ICO, controllers and processers [accessed on 8 July 2026].

[72] See ICO. Content moderation and data protection, in particular on What if we use automated decision-making in our content moderation? [accessed on 8 July 2026]. While the ICO's guidance on automated-decision making in content moderation is aimed at organisations who are carrying out content moderation to meet their obligations under the Online Safety Act, it explains that it also applies to organisations who are carrying out content moderation for other reasons.

ICO's guidance on "What does the UK GDPR say about ADM?"[73] explains that, in some situations, a human can set a simple rule that is applied automatically, but the system is not making its own separate decision.

2.255 We expect providers to implement our measures requiring them to identify known, validated scam URLs and numbers in messages using a database matching tool (where a human sets a rule that is applied automatically), rather than a system making decisions based on the likelihood of something happening. It is, however, providers' responsibility to ensure they comply with relevant data protection rules, taking into account how they implement our measures and the ICO's associated guidance. Where Article 22A applies, providers must ensure they comply with the restrictions and safeguards in Articles 22B-D UK GDPR.[74] The ICO has also published guidance on automated decision making and profiling. [75]

2.256 Other data protection legislation and guidance relating to monitoring of traffic data is particularly relevant to our rules. Providers should, for example, ensure they comply with Regulations 7, 8 and 29 of the PECR.

2.257 This is not intended to be an exhaustive list and providers are expected to take appropriate legal advice and ensure they comply with all data protection legislation that applies to them when complying with the GCs to which they are subject.

2.258 We are satisfied that providers can implement our rules in accordance with data protection law. As noted above, the ICO has published guidance on content moderation and data protection, which explains how data protection law applies to content moderation technologies and processes, including where these are solely automated, and provides advice to help service providers comply with the UK GDPR and the DPA when using these technologies and processes. This includes advising service providers to carry out a data protection impact assessment to assess and mitigate data processing risks.

2.259 As explained in paragraph 2.29 above, we note that data protection law is not a barrier to sharing data for fraud prevention but is a framework for doing so responsibly. The UK GDPR and DPA both contain specific provisions that support the sharing of personal data to prevent and detect crime, including fraud. The Data Use and Access Act further strengthened these foundations by amending the UK GDPR to introduce a new "recognised legitimate interests" basis for processing, which includes fraud prevention.[76]

2.260 Providers should also ensure they comply with their obligations under other legislation that may be relevant (see paragraph 1.15).

[73] ICO. What does the UK GDPR say about ADM? [accessed on 8 July 2026].
[74] ICO. What are the ADM safeguards? [accessed on 8 July 2026].
[75] ICO. Guidance on automated decision making and profiling [accessed on 8 July 2026].
[76] See, Article 6(1)(ea) and paragraph 5(a) of Annex 1 of the UK GDPR.

3. How we will enforce the rules

3.1 We have a range of powers to take enforcement action for non-compliance with our rules relating to scam mobile messages. We may decide to pursue more than one of these options in the particular circumstances of the case, as permitted by the relevant legislation.

3.2 When deciding whether to take enforcement action and what enforcement action may be the most appropriate, Ofcom will consider all relevant factors. This includes (but is not limited to) the available evidence that a provider is in breach of the relevant rule, including the extent to which a provider has taken into account the expectations in this guidance. We may obtain evidence from a variety of sources, which may include:

- Statutory information requests.
- Ofcom's own monitoring or intelligence. For example, we may consider it appropriate to apply to be a new customer of a provider, to check their KYC process is robust and reflects their relevant policy.
- Intelligence provided by a third party.

3.3 We are more likely to take action against a provider we consider primarily responsible for any non-compliance but may also take action against other providers we consider have failed to take appropriate steps to prevent that non-compliance.

3.4 Where applicable, any enforcement action will generally be carried out in line with Ofcom's Regulatory Enforcement Guidelines.[77]

General Conditions

3.5 We can take enforcement action under our GCs relating to scam mobile messages, including GC C9, as well as existing GCs including B1 and B4.4.

3.6 We may take action under more than one GC in the particular circumstances of the case. For example, a breach of GC C9 may also be considered a breach of GCs B1.6, 1.8 and/or 1.9.

3.7 Our powers to take enforcement action under our GCs relating to scam mobile messages include:

- Powers to impose significant financial penalties of up to 10% of annual turnover.[78]
- Powers to direct providers to take steps in order to comply with the relevant GC and/or remedy the consequences of the contravention. This could include, for example, directing a communications provider to: (i) take certain action in relation to a number, sender or message; or (ii) compensate persons that have suffered loss or damage as a result of the non-compliance.[79] It is the duty of the person to comply with any such direction and that duty is enforceable in civil proceedings by Ofcom.[80]

[77] Regulatory Enforcement Guidelines for investigations.
[78] See sections 96A-98 of the Act. We can impose any penalty we consider to be appropriate and proportionate up to the statutory cap and taking into account Ofcom's penalty guidelines.
[79] Section 96A(2)(d) and section 96C(2)(a) of the Act.
[80] Section 96C (5) and (6).

- Powers to suspend a communications provider's entitlement to provide electronic communications networks or electronic communications services, or to make associated facilities available.[81]
- Powers to issue a direction under GC B4.4 requiring communications providers to block access to certain numbers or communications services on the basis of fraud or misuse.[82]
- Powers to withdraw telephone number allocations if any of the conditions in section 61(1) of the Act are met including when withdrawal is in accordance with GC B1.18(d) or (e):
    - B1.18(d) gives us the power to withdraw numbers where "the Communications Provider has used a significant proportion of those Telephone Numbers, or has used such Allocation to a significant extent, inconsistently with … Condition [B1], or to engage in fraud or misuse". Depending on the nature and degree of harm that a scam or potential scam may cause, we may consider a single instance of misuse to constitute using an "Allocation to a significant extent, inconsistently with … Condition [B1], or to engage in fraud or misuse".
    - B1.18(e) gives us the power to withdraw numbers where "Ofcom has advised the Communications Provider in writing that a significant proportion of those Telephone Numbers has been used, or that such Allocation has been used to a significant extent, to cause harm or a nuisance, and the Communications Provider has failed to take adequate steps to prevent such harm or nuisance".

3.8 If we withdraw a +44 number, that number will no longer be allocated to a person, meaning providers should not carry traffic related to that number, even if it does not transit or terminate in the UK. We may take enforcement action under GC B1.3 against any UK provider that continues to carry such traffic.

Non-Provider Conditions

3.9 In the event of non-compliance with Non-Provider Condition 3, we have powers under section 59(6) of the Act to take enforcement action via civil proceedings against operators allocated numbers that may not be considered a communications provider within the scope of the GCs. We also have the power to withdraw numbers under section 61(4) of the Act.

Persistent misuse

3.10 Ofcom also has powers under sections 128 to 130 of the Act to take enforcement action against providers or other persons who persistently misuse an electronic communications network or services, including issuing a penalty of up to £2m. Misuse of an electronic communications network or service involves using a network or service in ways which cause or are likely to cause someone else (including consumers) to unnecessarily suffer annoyance, inconvenience or anxiety. Misuse is persistent where it is repeated enough for it to be clear that it represents a pattern of behaviour or practice, or recklessness about whether others suffer the relevant kinds of harm. Any enforcement action for Persistent Misuse would take into account Ofcom's Persistent Misuse statement.[83]

[81] Section 100 of the Act.
[82] See Annex A11 of our Regulatory Enforcement Guidelines for a summary of the relevant enforcement process.
[83] Statement of policy on the persistent misuse of an electronic communications network or electronic communications service.

3.11 Depending on the circumstances, we may take action against a provider or the person carrying out the misuse.[84]

Other action

3.12 Depending on the circumstances, we may consider it appropriate to take other action, including using soft enforcement tools. For example, we may consider it appropriate to maintain on our website a list of providers found in breach of our rules and/or a list of numbers and/or Sender IDs that have been associated with scams and that should not be used, transmitted or terminated in the UK.

[84] See paragraphs 1.19-1.20 of Ofcom's Persistent misuse statement.